

André Roberto Guerra

Considerações sobre a Utilização do Recurso Wake Up

**Florianópolis – SC
2002**

**UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA
COMPUTAÇÃO**

André Roberto Guerra

Considerações sobre a Utilização do Recurso Wake Up

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação

João Bosco da Mota Alves

Florianópolis, Novembro de 2002

Considerações sobre a Utilização do Recurso Wake Up

André Roberto Guerra

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação Área de Concentração Sistemas de Conhecimento e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Fernando Alvaro Ostuni Gauthier
Coordenador do curso

Banca Examinadora

João Bosco da Mota Alves
Orientador

Luiz Fernando Jacintho Maia
Membro da Banca

Ilson Wilmar Rodrigues Filho
Membro da Banca

Agradecimentos

A minha maravilhosa família, que me ajudou em todas as etapas deste trabalho, desde o início de minha formação.

Ao meu orientador e amigo Prof. João Bosco da Mota Alves, pelo apoio, incentivo, segurança e, principalmente pela orientação transmitidas.

A Faculdade de Ciências Sociais Aplicadas de Cascavel que tornou viável a realização dos créditos em Cascavel, a cidade que resido.

Aos Docentes do Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina, que se dispuseram a realizar este curso em Cascavel.

A Deus, mais uma vez, por me abençoar com conhecimento e força de constituir a empresa André Roberto Guerra Informática, que viabilizou os recursos necessários para o estudo e para todos os experimentos deste trabalho. Agradeço por ter colocado em meu caminho pessoas como Rogério Cid Bastos, Raul S. Wazlawick, Vítório B. Mazzola, Roberto Willrich, Murilo S. de Camargo, Jorge Muniz Barreto, José Eduardo DeLucca os docentes acima citados, que transmitiram tanto conhecimento, aqueles todos que, mesmo indiretamente, ajudaram a realizar este trabalho.

SUMÁRIO

SUMÁRIO.....	i
LISTA DE FIGURAS.....	iii
RESUMO.....	v
ABSTRACT.....	vi
 1. INTRODUÇÃO.....	 01
1.1 OBJETIVOS.....	03
1.1.1 Objetivos Gerais.....	03
1.1.1 Objetivos Específicos.....	03
1.2 RELEVÂNCIA.....	03
 2. SOFTWARE DE COMUNICAÇÃO.....	 04
2.1 UTILIDADES DO SOFTWARE.....	05
2.2 COMO O SOFTWARE FUNCIONA.....	06
2.2.1 Noções básicas sobre os termos Host e remoto.....	06
2.2.2 Noções básicas sobre o controle remoto.....	07
2.2.2.1 A diferença entre o controle remoto e a rede remota.....	07
2.3 SEGURANÇA.....	08
2.4 PERSONALIZAÇÃO.....	09
2.5 DESEMPENHO.....	09
 3. PROTOCOLOS.....	 11
3.1 MODELO OSI.....	13
3.1.1 Camada 7 – Aplicação.....	17
3.1.2 Camada 6 – Apresentação.....	18
3.1.3 Camada 5 – Sessão.....	18
3.1.4 Camada 4 – Transporte.....	18
3.1.5 Camada 3 – Rede.....	19
3.1.6 Camada 2 – Link de Dados.....	19
3.1.7 Camada 1 – Física.....	20
3.2 NDIS e ODI.....	20
 4. TCP/IP.....	 23
4.1 CAMADA DE APLICAÇÃO.....	24
4.2 CAMADA DE TRANSPORTE.....	25
4.3 CAMADA DE INTERNET.....	26
4.4 CAMADA DE INTERFACE COM A REDE.....	27
 5. APLICAÇÃO E DISCUSSÃO.....	 28
5.1 WAKE UP ON RING (WOR).....	28
5.2 PLACA MÃE ASUS P3B-F.....	29
5.3 PLACA MÃE PCCHIPS M756LMRT+.....	32

5.4 PLACA DE COMUNICAÇÃO IBM.....	34
5.5 INSTALAÇÃO E CONFIGURAÇÃO.....	34
5.4.1 Instalação e Configuração do Software.....	35
CONCLUSÃO.....	51
GLOSSÁRIO.....	52
REFERÊNCIAS BIBLIOGRÁFICAS.....	57

LISTA DE FIGURAS

Figura 01. Exemplo de um pacote de dados.....	13
Figura 02. Modelo OSI de protocolos.....	14
Figura 03. Funcionamento da comunicação entre as camadas OSI.....	15
Figura 04. Comunicação virtual do modelo OSI.....	16
Figura 05. Grupos das camadas do modelo OSI.....	16
Figura 06. Arquitetura do TCP/IP.....	23
Figura 07. Funcionamento da camada de Aplicação.....	25
Figura 08. Funcionamento do TCP/IP.....	27
Figura 09. Conector Wake Up On Modem.....	28
Figura 10. Manual placa mãe ASUS.....	30
Figura 11. Manual placa mãe ASUS.....	31
Figura 12. BIOS.....	31
Figura 13. Manual placa mãe ASUS.....	32
Figura 14. Descrição placa mãe PCChips M756LMRT+.....	33
Figura 15. Tela inicial do Symantec pcAnywhere	35
Figura 16. Tela <i>Install</i>	36
Figura 17. Tela de alerta do pcAnywhere.....	37
Figura 18. Tela de Boas vindas do assistente para instalação do pcAnywhere.....	37
Figura 19. Contrato de licença de uso do Symantec pcAnywhere.....	38
Figura 20. Informações sobre o cliente.....	39
Figura 21. Tipo de instalação.....	40
Figura 22. Tela de início da instalação.....	40
Figura 23. Soluções de Suporte.....	41
Figura 24. LiveUpdate.....	41
Figura 25. Conclusão da Instalação.....	42
Figura 26. Tela Inicial do Symantec pcAnywhere.....	43
Figura 27. Propriedades da conexão <i>Host</i>	44
Figura 28. Preferências do dispositivo de conexão.....	45
Figura 29. Configurações adicionais do <i>Host</i>	46

Figura 30. Configurações adicionais do <i>Host</i> – quem conecta.....	47
Figura 31. Privilégios do discador.....	48
Figura 32. Opções de segurança do <i>Host</i>	49

RESUMO

Os microcomputadores atuais, em sua grande maioria, possuem um recurso *Built-In* (Integrado) entre placa principal (Placa Mãe) e a placa de comunicação (Modem ou Rede) denominado *Wake Up*, em sua tradução “Acordar” onde, ao receber uma chamada pela rede ou uma chamada telefônica, a placa de Rede ou o Modem são capazes de ligar o computador e iniciar o serviço de comunicação.

Neste trabalho é proposto um modelo para desenvolvimento de aplicações que utilizam esse recurso. O modelo contempla o funcionamento dos dispositivos de Hardware e Software necessários, sua instalação e configuração, bem como algumas implicações no que tange a segurança. Um exemplo de utilização do recurso foco da dissertação ilustra as principais características do modelo do recurso acima citado.

Palavras-Chave: 1.Protocolos, 2.TCP, 3.Wake Up.

ABSTRACT

Most of the present microcomputers have a Built In resource between the Mother Board and the Communication Card (Modem or LAN) named Wake Up, which means, when the Communication Card receives a calling it can be able to turn the computer on and start the Communication service. This paper proposes a model in order to develop applications to make use of this resources. The model has considered the performance of the Hardware and the Software devices, which are necessary, its installation an configuration, as well any implications concerning security. Finally, an example of utilization shows the main characteristics of the Resource Model Mentioned above.

Keywords: 1. Protocols, 2. TCP/IP, 3.Wake Up.

1. INTRODUÇÃO

Os avanços tecnológicos sempre crescentes na microeletrônica e nas comunicações, a necessidade do compartilhamento de recursos (hardware e software) e a tendência crescente de descentralização geográfica e funcional do uso de computadores ocasionaram o surgimento das Redes de Computadores. As Redes de Computadores são caracterizadas por um conjunto de computadores autômatos (cada processador tem poder de decisão) e interconectados (capazes de trocar informações) [TANEMBAUM, 1994].

A maioria das placas-mãe hoje em dia possui esses recursos. O computador pode ser configurado para entrar em um modo chamado "*stand by*", onde ele é aparentemente desligado, mas a sua memória RAM continua sendo alimentada. Com isso, o sistema operacional e os programas continuam carregados. Ao ser "acordado" o microcomputador já estará com o sistema operacional carregado e com os programas que estavam abertos. O *wake up* é um recurso que permite ao microcomputador "acordar" caso alguma outra máquina o chame através da rede ou então através do modem. Isso permite, por exemplo, que o microcomputador esteja "desligado" esperando ligações de fax, caso o mesmo possua um programa que permita receber faxes. Assim, em vez de o micro ficar ligado consumindo energia elétrica, ele ficará "desligado", economizando energia. Percebe-se que, na verdade o micro não estará "desligado", mas sim em um estado de "hibernação" (*stand by*). [TORRES, 2001]

Esse recurso permite que computadores sejam ligados e desligados remotamente através da linha telefônica ou da rede. Assim, pode-se ligar, acessar e desligar um computador que esteja localizado a quilômetros de distância do usuário. Para esse recurso funcionar, tanto a placa de comunicação quanto a placa-mãe devem suportá-lo e devemos ligar a placa de comunicação à placa-mãe através de um cabo com dois fios, em um conector apropriado na placa-mãe (marcado com "*Wake Up*" ou similar). Além disso, o modem deverá estar ligado à linha telefônica ou a rede e programado para receber chamadas.

Um software deverá estar habilitado na máquina para permitir o acesso externo - como o Servidor *Dial Up* do Windows 98 -, de modo que se consiga acessar a máquina remotamente (obviamente esse acesso é feito através de um pedido de login e senha). [ATSERVIÇOS, 2002]

É praticamente impossível hoje em dia não pensar em redes quando o assunto é informática. Basta lembrar que grande parte das pessoas compra computadores hoje para ter acesso a maior das redes existentes – a Internet. [TORRES, 2001]

A comunicação, a interconexão entre os computadores através das Redes de Computadores, torna-se uma ferramenta de fundamental importância.

Com a queda do custo de implementação de redes, é praticamente impossível pensar em um ambiente de trabalho em que os computadores existentes não estejam interligados, por menor que seja esse ambiente. Mesmo em pequenos escritórios com apenas dois micros a necessidade de uma rede torna-se evidente quando é necessário ficar levando disquetes para lá e para cá contendo arquivos de trabalho, ainda mais se esses arquivos forem grandes e não couberem em um só disquete, o que é cada vez mais comum. [TORRES, 2001]

Além da facilidade de se trocar dados, existem ainda inúmeras outras vantagens, como o compartilhamento de recursos e serviços.

Deve-se, porém tomar muito cuidado na escolha do profissional a executar este serviço. É necessário um profissional com boa formação, com cursos de certificação, pois, são as informações, os dados do usuário que serão disponibilizados, sendo necessário um bom Sistema Operacional de Rede para a administração dos compartilhamentos, um cuidado extra com a segurança das informações, bem como a correta configuração dos mesmos para se obter o total êxito, ou seja, pessoas e empresas visam à implementação de uma rede tendo em vista o aumento da produtividade do trabalho, basicamente por dois motivos:

- Troca de dados (arquivos, informações, aplicativos, etc).
- Acesso a recursos (Software e Hardware) Este é o objetivo principal deste trabalho.

Na Internet, essa troca de informações armazenadas remotamente é levada ao extremo: são acessados dados que estão armazenados nos locais mais remotos e, na maioria das vezes, o local onde os dados estão fisicamente armazenados não tem a menor importância. [TORRES, 2001]

1.1 OBJETIVOS

1.1.1 Objetivos Gerais

O objetivo deste trabalho é apresentar uma explicação detalhada desse recurso, *Wake up*.

1.1.2 Objetivos Específicos

- Estudar os recursos de Hardware e Software
- Apresentar um exemplo de uso desse recurso.
- Validar o uso deste recurso aqui apresentado.

1.2 RELEVÂNCIA

Por tratar-se de uma dissertação de mestrado e de um assunto paupérrimo em referências bibliográficas, com pouquíssimos estudos concluídos, podem existir outros estudos que abordem temas aqui citados.

Esta dissertação trata de um tema muito fechado com pouquíssimo referencial teórico conceitual, sendo utilizado em grande parte de estudos práticos. Para que se tenha um conhecimento mais amplo de tais tópicos será necessário um estudo mais aprofundado dos referidos tópicos. Todo tópico aqui abordado servirá de base para estudos futuros.

O Software utilizado no exemplo de uso é um software proprietário, detalhado em um capítulo específico, baseado em plataformas também proprietárias, tornando assim, de valor muito elevado a utilização dos mesmos.

A presente dissertação propõem então um estudo futuro no que tange o desenvolvimento de um software livre.

A necessidade cada vez maior de ter acesso ao dados torna esse estudo de fundamental importância, pois o que aqui é proposto é o acesso, o compartilhamento, o uso do equipamento, mesmo que esteja distante fisicamente e “desligado”, isso tudo com segurança e velocidade satisfatórias.

2. SOFTWARE DE COMUNICAÇÃO

Será neste capítulo abordado o software de comunicação a se utilizar para o compartilhamento de recursos de Hardware e Software entre os computadores conectados. Como explicado no Capítulo 1 deste trabalho, uma das relevâncias deste é justamente a questão do software utilizado, pois o mesmo é um Software proprietário baseado em plataformas também proprietárias, tornando assim de alto custo a utilização do recurso aqui estudado. Este trabalho serve de referencial teórico conceitual para estudos futuros, pois aqui se abre um espaço para a criação de um Software livre baseado em plataformas também livres. Será apresentado aqui um Software proprietário bastante completo, com muitos recursos e de ótima segurança.

Foram pesquisados alguns Softwares livres como o VNC, a se utilizar em plataforma livre ou proprietária. Porém o referido, mesmo com a vantagem de ser um Software livre, é bastante limitado, com poucos recursos.

Foi também estudada a plataforma (Sistema Operacional) FreeBSD e este também é compatível com o recurso, mas, por ser uma plataforma livre, necessita de altíssimo grau de instrução do mesmo, fazendo-se necessário um estudo detalhado do mesmo, pois não existe nada pronto.

A relevância dos softwares citados, a falta de recursos, de documentação e de suporte tornaram decisiva a escolha do software apresentado.

Considerando-se os pontos relevantes relacionados aos softwares anteriormente citados, optou-se então pela escolha do Symantec PcAnywhere. Ao serem analisadas situações como a de um funcionário que trabalha em sua casa e faz seus negócios por telefonia, um profissional de negócios que viaja com frequência ou um profissional de informática que suporta computadores de outros usuários remotamente, é bem provável que precise acessar outro computador de um local remoto. Pode-se estar trabalhando com uma apresentação em casa e perceber que precisa de informações de um arquivo que está na unidade de disco do seu computador no escritório, ou talvez possa estar tentando ajudar um cliente de outra cidade com um problema de software e precisa saber o que está acontecendo pela tela do computador desse cliente.

Permite conectar-se remotamente a outro computador, abrir qualquer arquivo ou programa aos quais tenha permissão de acesso, e trabalhar como se estivesse sentado defronte do mesmo computador.

Inclui um número de novos recursos e ferramentas do administrador, projetados para aumentar a segurança, otimizar o desempenho e facilitar o uso e a personalização do software.

Por tudo isso e principalmente por suportar o recurso aqui estudado, oferecendo tudo o que é preciso de um software de comunicação *Peer-to-peer*, esse foi o software escolhido o Symantec PcAnywhere que nesse capítulo será afundo explicado.

2.1 UTILIDADES DO SOFTWARE

São apresentadas neste capítulo algumas vantagens na utilização do Software escolhido e estudado.

- **Resolução de problemas do computador.** Os operadores de “*helpdesk*”, administradores de rede e outros profissionais de informática usam o pcAnywhere para conectar-se remotamente a outro computador e resolver os problemas. Permite a visualização da tela de outro computador, verificar e modificar as configurações, e reiniciar o computador — tudo isso de seu computador.
- **Suportando e mantendo servidores.** Os administradores de rede podem usá-lo para se conectar a servidores dentro de suas organizações e executar a manutenção de rotina, avaliar o desempenho e resolver os problemas de rede.
- **Recuperando arquivos de computadores domésticos ou no escritório.** É possível conectar-se ao computador em casa ou no escritório para obter rapidamente os arquivos que precisa.
- **Trabalhando de um local remoto.** Permite a conexão a outro computador e a execução de tarefas como se estivesse à frente do mesmo. Pode-se visualizar e editar arquivos, acessar recursos de rede, executar programas e imprimir arquivos os quais tenha permissão.

2.2 COMO O SOFTWARE FUNCIONA

Usa a tecnologia de controle remoto para permitir a conexão a outro computador ou a uma rede de área local (LAN, *local area network*) e trabalhar como se estivesse sentado na frente do mesmo computador. Para estabelecer uma conexão, os dois computadores devem estar executando o pcAnywhere. Um computador deve ser configurado como o *Host*, e o outro como o remoto. Um novo usuário, deverá saber a diferença entre um computador *Host* e remoto antes de começar.

2.2.1 Noções básicas sobre os termos *Host* e remoto

O relacionamento entre um computador *Host* e remoto é semelhante a um aparelho de televisão e um dispositivo de controle remoto. Usando o dispositivo de controle remoto, é possível ajustar o volume, mudar de canal, ligar ou desligar a televisão sem sair do sofá. Usando o pcAnywhere, um computador *Host* aguarda e aceita conexões do computador remoto e executa as funções solicitadas, da mesma forma em que o aparelho de televisão aceita os sinais de um dispositivo de controle remoto.

Antes que os dois computadores se conectem um com o outro, um deles deve ser configurado como o *Host* e o outro como o remoto. O computador *Host* aguarda por conexões de um computador remoto e permite que seja controlado. Ao configurar um computador *Host*, controla-se quem pode se conectar ao seu computador e qual o nível de acesso que o usuário remoto deve ter. Por exemplo, é possível impedir que um usuário remoto reinicie seu computador.

O computador remoto se conecta ao *Host* e especifica as ações que devem ser executadas. Embora o trabalho real seja executado no computador *Host*, qualquer coisa que aconteça na tela do *Host* será exibida na tela do computador remoto também. Esta troca entre os computadores remoto e *Host* é chamada de sessão de controle remoto.

2.2.2 Noções básicas sobre o controle remoto

A tecnologia de controle remoto permite a conexão a um computador *Host* de seu local remoto e a utilização do *Host* como se o usuário estivesse sentado na frente dele. Caso esteja se conectando a um computador *Host* na rede, poderá acessar qualquer arquivo ao qual o *Host* tenha permissão de acesso.

O controle remoto é mais rápido e eficiente que as outras formas de rede remota, principalmente se precisar usar um programa de software no computador *Host*. Quando executado um programa de software durante uma sessão de controle remoto, o processamento real é executado no computador *Host*. Apenas as informações de entrada e saída (por exemplo, teclado, mouse e informações da tela) são trocadas entre os computadores remoto e *Host*.

Por exemplo, caso esteja usando um programa de planilha eletrônica para atualizar seu relatório de despesas mensais, os cálculos matemáticos serão executados no computador *Host*, e apenas os resultados dos cálculos serão enviados ao computador remoto. Pelo fato de apenas os dados mínimos precisarem ser transferidos entre os dois computadores, o controle remoto resulta em um melhor desempenho e minimiza o risco de perda de dados.

2.2.2.1 A diferença entre o controle remoto e a rede remota

A rede remota permite a conexão do usuário a uma rede discando por um servidor de rede, se estiver usando um modem e não puder se conectar a uma rede diretamente. É freqüentemente denominada como rede *Dial-Up* nos sistemas Windows 9x e Windows ME ou serviço de acesso remoto (RAS, *remote access service*) nos sistemas Windows NT e Windows 2000.

Durante uma sessão de rede remota, o computador remoto trabalha como se estivesse diretamente conectado à rede. Será possível acessar apenas os arquivos e programas da rede em que o administrador de rede tiver concedido permissão de acesso ao usuário remoto. Ao executar um programa de software durante uma sessão de rede remota, o processamento ocorrerá no computador remoto.

Todas as informações e os dados solicitados pelo programa devem ser comunicados pela linha telefônica ao computador remoto. Mesmo com *modems* de alta velocidade, as linhas telefônicas são muito mais lentas que as conexões LAN diretas principalmente se precisarem acessar um arquivo ou programa grande.

2.3 SEGURANÇA

A atenção na segurança foi reforçada para ajudar os usuários a protegerem seus computadores do acesso não autorizado e para ajudar os administradores de rede e profissionais de segurança a identificarem e impedirem falhas na segurança, pois, no que tange a segurança, as plataformas ou sistemas operacionais são muito ineficientes.

Novos métodos de autenticação para plataformas baseadas na Microsoft, Novell e Web. Os novos métodos de autenticação incluem: Serviços de diretório ativo (ADS, *Active Directory Service*), FTP, HTTP, HTTPS, LDAP (*Lightweight Directory Access Protocol*), Serviço do Novell Bindery e NDS (*Novell Directory Service*).

A segurança do *Host* agora exige senhas para efetuar *login* no *Host*. O usuário *Host* deve escolher um método de autenticação e configurar contas de usuários remotos para usuários remotos ou grupos de usuários.

A capacidade de rastrear arquivos e executáveis abertos durante uma sessão do *Host*, para segurança adicional.

Os usuários do Windows NT e Windows 2000 também podem rastrear os eventos do registro do pcAnywhere no Visualizador de eventos.

Remote Access Perimeter Scanner (RAPS). Esta nova ferramenta do administrador verifica se há *Hosts* sem segurança na rede da empresa e detecta a presença de vários produtos de acesso remoto conhecidos para identificar possíveis riscos de segurança.

A capacidade de travar as configurações para impedir interferências nos arquivos, nos executáveis e nas configurações do registro.

A capacidade de proteger a segurança da configuração, usando o gerenciamento de diretivas. O gerenciamento de diretivas permite que os administradores escolham quais itens de interface do usuário os usuários podem visualizar ou modificar. Esse recurso está disponível apenas para o Windows NT e Windows 2000.

2.4 PERSONALIZAÇÃO

Proporciona mais flexibilidade aos administradores para personalização do sistema de acordo com as necessidades do usuário. Os novos recursos de personalização incluem:

- *Packager*. Com ele os administradores podem criar e disponibilizar conjuntos de instalações personalizados para aprimorar a segurança e o desempenho ou reduzir o espaço em disco necessário para instalar ou executar o pcAnywhere. Esse recurso está disponível apenas para o Windows NT e Windows 2000.
- Ferramenta de instalação da Web. Permite que os administradores disponibilizem o pcAnywhere na Internet ou na intranet corporativa.
- Pacotes de instalação pré-configurados. Os administradores podem instalar esses pacotes ou usá-los como modelos para criação de seus próprios pacotes de instalação personalizados.
- Automação de vinculação e incorporação de objetos (OLE, *Object linking and embedding*). Permite que os administradores gravem aplicativos para automatizar determinadas funções no pcAnywhere.

2.5 DESEMPENHO

A janela principal foi criada para facilitar a navegação e diferenciar entre os modos *Host* e remoto. Os aprimoramentos de desempenho incluem:

- Assistente de otimização guia o usuário pelas etapas de otimização de uma conexão, destacando as opções disponíveis para aprimoramento do desempenho e informando aos usuários sobre os prós e contras entre o desempenho e a segurança.
- Aprimoramentos do gerenciador de arquivos que facilitam a localização e seleção dos arquivos e pastas para transferência de arquivos.
- O menu Ir permite a navegação rápida até as pastas e arquivos visitados recentemente.

- Os recursos de rotulação permitem selecionar arquivos e pastas rapidamente para transferência ou sincronização de arquivos. Pode usar os padrões de caracteres curingas para rotular arquivos e pastas.

A capacidade dos usuários ISDN CAPI de selecionarem união de canais ao usarem o recurso de retorno de conexão do *Host*. Esta versão também trata de questões de desempenho envolvendo a união de canais CAPI. [SYMANTEC, 2001]

Com toda a explicação apresentada neste capítulo, fica fácil entender o porque da escolha deste Software de Comunicação. Agora se tem base, referencial teórico conceitual para iniciar um estudo maior e mais detalhado sobre as plataformas livres para então desenvolver um Software tão bom quanto o aqui apresentado para que se faça uso do recurso *Wake Up*.

3. PROTOCOLOS

Um dos assuntos mais importantes em relação a redes locais é o referente a protocolos. São os protocolos que definem como a rede irá funcionar de verdade, pois são eles que definem como os dados enviados por programas serão transferidos pela rede. [COMMER] Portanto, para entendermos a fundo como as redes locais funcionam, devemos dominar com clareza esse assunto.

Protocolo é a “linguagem” usada pelos dispositivos de uma rede de modo que eles consigam se entender, isto é, trocar informações entre si. Para que todos os dispositivos de uma rede consigam conversar entre si, todos eles deverão estar usando uma mesma linguagem, isto é, um mesmo protocolo.

Uma rede pode usar diversos protocolos, como o TCP/IP, o NetBEUI e o IPX/SPX, entre outros, mas neste trabalho será dada ênfase ao protocolo TCP/IP, cujo funcionamento será explicado de maneira ampla.

Embora cada um destes protocolos funcione de uma forma particular, eles tem algumas similaridades, que existem porque, na verdade, todos os protocolos têm um mesmo objetivo que é a transmissão de dados em uma rede.

Para entender melhor como os protocolos funcionam, considerem-se as seguintes premissas:

- A maioria das transmissões de dados em redes locais é do tipo *half-duplex*;
- Mesmo em redes que utilizam hubs, onde cada microcomputador é conectado à rede usando um cabo individual, esse componente na verdade funciona apenas como um repetidor, enviando para todas as máquinas da rede as informações que recebe, ao mesmo tempo.
- Se uma transmissão está sendo feita entre dois dispositivos, nenhuma outra transmissão poderá ser feita ao mesmo tempo, mesmo que seja entre outros dois componentes diferentes que não estejam participando da transmissão em curso.
- Se um arquivo grande precisar ser transmitido, os demais dispositivos da rede terão de esperar muito tempo para começarem a transmitir, pois o arquivo é grande e demora algum tempo para ser transmitido.

- Poderão ocorrer interferências de algum tipo no meio do caminho e o dado pode não chegar corretamente ao seu destino.

Os protocolos são justamente uma solução para todos estes problemas. Primeiro, o protocolo pega os dados que devem ser transmitidos na rede dividindo-os em pequenos “pedaços” de tamanho fixo chamados pacotes ou quadros. Isto significa que um arquivo não é transmitido na rede de uma só vez. Dentro de cada pacote há uma informação de endereçamento que informa a origem e o destino do pacote. As placas de rede dos computadores possuem um endereço fixo, que é gravado em hardware. Dessa forma, o computador de destino sabe que o pacote atualmente transmitido é para ele, porque há o endereço de sua placa de rede no cabeçalho de destino do pacote e da mesma forma, os demais computadores sabem que aquele pacote não é para eles. [TORRES]

O uso de pacotes de dados otimiza enormemente o uso da rede, já que, em vez de uma única transmissão de um dado grande, existirão várias transmissões de dados menores. Com isso, estatisticamente haverá uma maior probabilidade de um outro dispositivo que queira transmitir um dado encontrar espaço para iniciar uma nova transmissão. Dessa forma é possível que vários dispositivos se comuniquem “ao mesmo tempo” em uma rede. Fisicamente, essas transmissões não são efetuadas simultaneamente, mas intercalando os vários pacotes de dados. A velocidade de transmissão de dados em uma rede é altamente dependente do número de transmissões simultâneas efetuadas.

Finalizando, a placa de rede, ao colocar um pacote de dados no cabo da rede, cria uma conta chamada *checksum* ou *CRC (Cyclical Redudancy Check)*. Essa conta consiste em somar todos os *bytes* presentes no pacote de dados e enviar o resultado dentro do próprio pacote. [CYCLADES] A placa de rede do dispositivo receptor irá refazer esta conta e verificar se o resultado calculado corresponde ao valor enviado pelo dispositivo transmissor. Se os valores forem iguais, significa que o pacote chegou íntegro ao seu destino.

Caso contrário, significa que houve algo de errado na transmissão (uma interferência no cabo, por exemplo) e os dados recebidos são diferentes dos originalmente enviados, ou seja, os dados chegaram corrompidos ao destino.

Neste caso, o dispositivo receptor pede ao transmissor uma retransmissão do pacote defeituoso. Essa é outra vantagem de se trabalhar com pequenos pacotes em vez de transmitir diretamente o arquivo.

Endereço de Destino	Endereço de Origem	Informações de controle	Dados	CRC
---------------------	--------------------	-------------------------	-------	-----

Figura 01 – Exemplo de um pacote de dados

3.1 MODELO OSI

Quando as redes de computadores surgiram, as soluções eram, em sua maioria, proprietárias, isto é, uma determinada tecnologia só era suportada por seu fabricante. Não havia a possibilidade de se misturar soluções de fabricantes diferentes. [BRISA & EMBRATEL] Dessa forma, um mesmo fabricante era responsável por construir praticamente tudo na rede.

“Para facilitar a interconexão de sistemas de computadores, a ISO (*International Standards Organization*) desenvolveu um modelo de referência chamado OSI (*Open Systems Interconnection*), para que os fabricantes pudessem criar seus protocolos a partir desse modelo.” [BRISA & EMBRATEL]

Interessante notar que a maioria dos protocolos existentes, principalmente o TCP/IP, que como dito anteriormente, será explicado de maneira mais ampla e completa, não segue esse modelo de referência ao pé da letra, só corresponde a partes do padrão OSI. Todavia, o estudo deste modelo é extremamente didático, pois através dele há como entender como deveria ser um “Protocolo ideal”, além de facilitar muito a comparação do funcionamento de protocolos criados por diferentes fabricantes.

O modelo de protocolos OSI é um modelo de sete camadas, apresentados na figura 02



Figura 02 – Modelo OSI de protocolos

Na transmissão de um dado, cada camada pega as informações passadas pela camada superior, acrescenta informações pelas quais ela seja responsável e passa os dados para a camada imediatamente inferior, como representado na figura 03. Esse processo é conhecido como encapsulamento. Na camada 4, Transporte, o dado enviado pelo aplicativo é dividido em pacotes. Na camada 2, Link de Dados, o pacote é dividido em quadros. Na recepção de um dado, o processo é inverso.

Um usuário que pede para o seu programa de correio eletrônico baixar seus e-mails, na verdade está fazendo com que o programa inicie uma transmissão de dados com a camada 7 – Aplicação – do protocolo usado, pedindo para baixar os e-mails do servidor correspondente. Essa camada processa esse pedido, acrescenta informações de sua competência, e passa os dados para a camada imediatamente inferior, a camada 6 (Apresentação). Esse processo continua até a camada 1 (Física) enviar o quadro de dados para o cabeamento da rede, quando, então, atingirá o dispositivo receptor, que fará o processo inverso, até a sua aplicação – no nosso exemplo, um programa servidor de e-mail.

A comunicação estudada na figura 03 é a comunicação real, ou seja, como funciona a transmissão de um dado através de uma rede. Na prática, acabamos simplificando e falando que uma determinada camada do transmissor comunica-se diretamente com a mesma camada do dispositivo receptor. Por exemplo, a camada 4, Transporte, do dispositivo transmissor comunica-se diretamente com a camada 4 do dispositivo receptor e simplesmente ignoramos as comunicações efetuadas pelas camadas inferiores existentes, e assim por diante.

Essa comunicação virtual, ilustrada na figura 04, é possível porque cada camada, durante a criação do pacote que será enviado através da rede, acrescentou seu próprio cabeçalho, como ilustrado na figura 03.

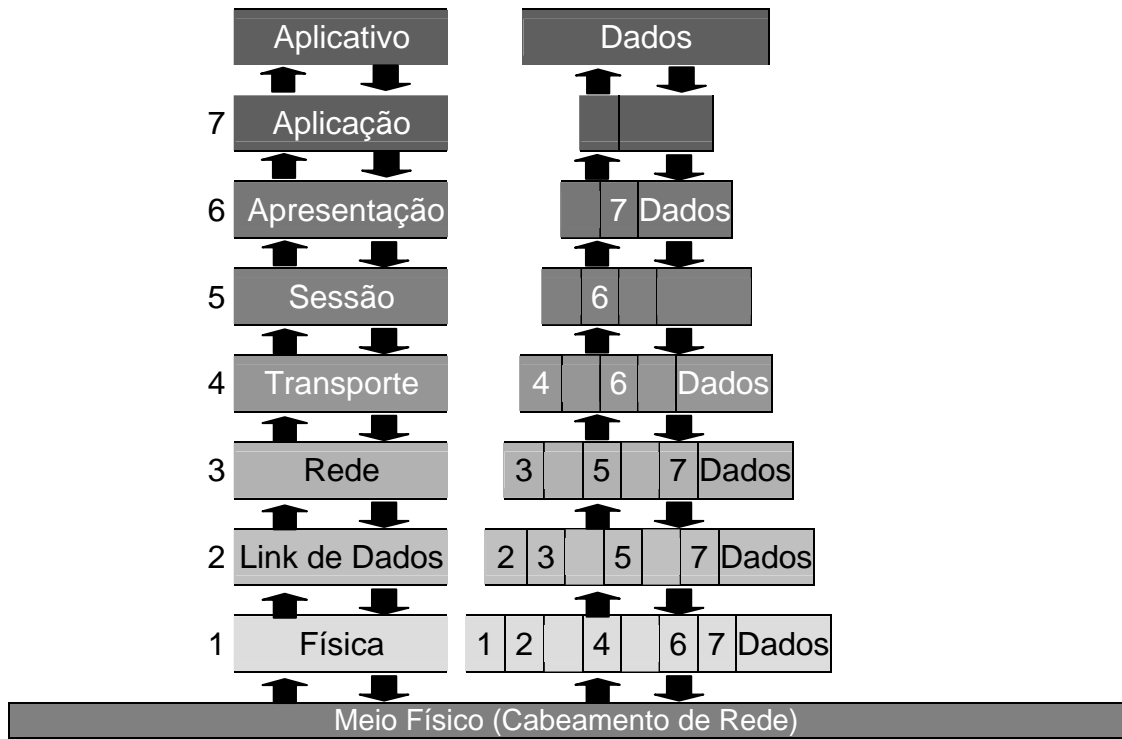


Figura 03– Funcionamento da comunicação entre as camadas OSI

Por exemplo, na prática simplesmente falamos que um programa cliente de e-mail está requisitando dados de um programa servidor de e-mail, e não nos preocupamos muito como isto é feito. O mesmo ocorre na comunicação virtual do modelo OSI. Quando analisamos a comunicação de uma camada do transmissor com a mesma camada no receptor, normalmente não estamos nos preocupando (ou não precisamos saber) como está ocorrendo a comunicação nas camadas inferiores àquela estudada.

A maioria dos protocolos, em especial o TCP/IP, também trabalha com o conceito de camadas, porém essas camadas não necessariamente possuem o mesmo nome e função das apresentadas no modelo OSI. [BRISA & EMBRATEL]

Muitas vezes, para cada uma dessas camadas há um protocolo envolvido. Dessa forma, muitos protocolos são, na verdade, um conjunto de protocolos, cada um com seu papel específico em sua estrutura de camadas.

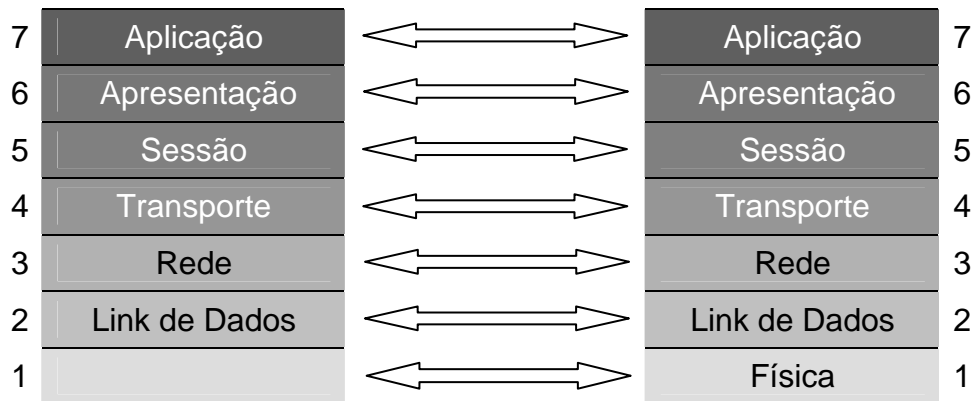


Figura 04 – Comunicação virtual do modelo OSI

As camadas do modelo OSI podem ser divididas em três grupos: aplicação, transporte e rede, como conferimos na figura 05. As camadas de rede se preocupam com a transmissão e recepção dos dados através da rede e, portanto, são camadas de baixo nível. A camada de transporte é responsável por pegar os dados recebidos pela rede e repassá-los para as camadas de aplicação de uma forma compreensível, isto é, ele pega os pacotes de dados e transforma-os em dados quase prontos para serem usados pela aplicação. As camadas de aplicação, que são camadas de alto nível, colocam o dado recebido em um padrão que seja compreensível pelo programa (aplicação) que fará uso deste dado.

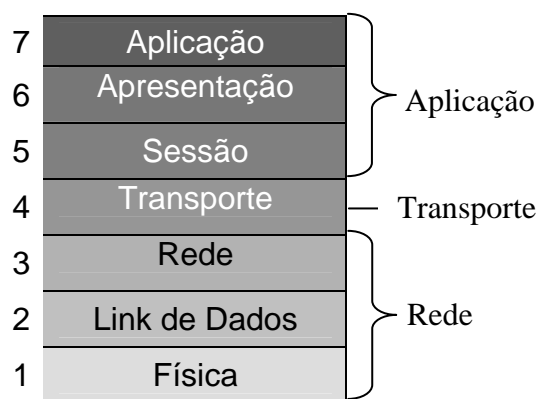


Figura 05 – Grupos das camadas do modelo OSI

Pacotes e quadros, até então, eram usados como sinônimos, mas estes termos se referem a duas coisas distintas. Um quadro é um conjunto de dados enviado através da rede, de forma mais “bruta” ou, melhor dizendo, de mais baixo nível. Dentro de um quadro encontramos informações de endereçamento físico, como, por exemplo, o endereço real de uma placa de rede. Logo, um quadro está associado às camadas mais baixas (1 e 2) do modelo OSI.

Um pacote de dados refere-se a um conjunto de dados manipulados nas camadas 3 e 4 do modelo OSI. No pacote há informações de endereçamento virtual. Por exemplo, a camada 4 cria um pacote de dados para ser enviado pela rede e a camada 2 divide esse pacote em vários quadros que serão efetivamente enviados através do cabo da rede. Um pacote, portanto, contém a informação proveniente de vários quadros.

Para dar um exemplo real e elucidar de uma vez essa diferença, em uma rede usando o protocolo TCP/IP, a camada IP adiciona informações de endereçamento de um pacote (número de endereço IP da máquina destino), que é um endereçamento virtual. Já a camada de controle de acesso ao meio (MAC) – que corresponde a camada 2 do modelo OSI – transformará esse pacote em um ou mais quadros e esses quadros terão o endereço da placa de rede de destino (endereço real, físico) que corresponda ao número IP fornecido. [ALBUQUERQUE]. Este protocolo será explicado de maneira mais ampla, deixando assim essa idéia mais clara e lúcida.

Serão explicadas agora, cada uma das camadas do modelo OSI e suas funções. Explicações definidas usando a transmissão de um dado do computador A para o computador B e o processo de recepção é o inverso do descrito.

3.1.1 CAMADA 7 - APLICAÇÃO

A camada de aplicação faz a interface entre o protocolo de comunicação e o aplicativo que pediu ou receberá a informação através da rede. Por exemplo, ao solicitar a recepção de e-mails através do aplicativo de e-mail, este entrará em contato com a camada de Aplicação do protocolo de rede efetuando tal solicitação.

3.1.2 CAMADA 6 – APRESENTAÇÃO

A camada de Apresentação, também chamada camada de Tradução, converte o formato do dado recebido pela camada de Aplicação em um formato comum a ser usado na transmissão desse dado, ou seja, um formato entendido pelo protocolo usado. Pode ter outros usos, como compressão e criptografia.

A compressão de dados pega os dados recebidos da camada 7 e os comprime e a camada 6 do dispositivo receptor fica responsável por descompactar esses dados. A transmissão dos dados torna-se mais rápida devido a existência de um número menor de dados a serem transmitidos, pois, os dados recebidos da camada 7 foram comprimidos e enviados a camada 5.

Para aumentar a segurança, pode-se usar criptografia neste nível, sendo que os dados só serão decodificados na camada 6 do dispositivo receptor.

3.1.3 CAMADA 5 - SESSÃO

A camada de Sessão permite que duas aplicações em computadores diferentes estabeleçam uma sessão de comunicação. Nesta sessão, essas aplicações definem como será feita a transmissão de dados e colocam marcações nos dados que estão sendo transmitidos. Se por ventura a rede falhar, os computadores reiniciam a transmissão dos dados a partir da última marcação recebida pelo computador receptor.

3.1.4 CAMADA 4 - TRANSPORTE

A camada de Transporte é responsável por pegar os dados enviados pela camada de Sessão e dividi-los em pacotes que serão transmitidos pela rede, ou melhor dizendo, repassados para a camada de Rede. No receptor, a camada de Transporte é responsável por pegar os pacotes recebidos da camada de Rede e remontar o dado original para enviá-lo à camada de Sessão. Isso inclui controle de fluxo (colocar os pacotes recebido em ordem, caso eles tenham chego fora de ordem) e correção de erros, tipicamente enviando para o transmissor uma informação de recebimento (*acknowledge*), informando que o pacote foi recebido com sucesso.

A camada de Transporte separa as camadas de nível de aplicação (camadas 5 a 7) das camadas de nível físico (camadas de 1 a 3). As camadas de 1 a 3 estão preocupadas com a maneira com que os dados serão transmitidos pela rede. Já as camadas de 5 a 7 estão preocupados com os dados contidos nos pacotes de dados, para serem enviados ou recebidos para a aplicação responsável pelos dados. A camada 4, Transporte, faz a ligação entre esses dois grupos.

3.1.5 CAMADA 3 - REDE

A camada de Rede é responsável pelo endereçamento dos pacotes, convertendo endereços lógicos em endereços físicos, de forma que os pacotes consigam chegar corretamente ao destino. Essa camada também determina a rota que os pacotes irão seguir para atingir o destino, baseada em fatores como condições de tráfego da rede e prioridades.

Essa camada é usada quando a rede possui mais de um segmento e, com isso, há mais de um caminho para um pacote de dados trafegar da origem ao destino, o que explica o porquê dos pacotes ocasionalmente serem recebidos fora de ordem.

3.1.6 CAMADA 2 – LINK DE DADOS

A camada de Link de Dados (também chamada de camada de Enlace) pega os pacotes de dados recebidos da camada de Rede e os transforma em quadros que serão trafegados pela rede, adicionando informações como o endereçamento da placa de rede de origem, o endereçamento da placa de rede de destino, dados de controle, os dados em si e o CRC. A estrutura do pacote de dados criado por esta camada é a representada na figura 03.

O quadro criado pela camada Link de Dados é enviado para a camada Física, que converte esse quadro em sinais elétricos para serem enviados através do cabo de rede.

Quando o receptor recebe um quadro, a sua camada Link de Dados confere se o dado chegou íntegro, refazendo o CRC. Se os dados estão corretos, ele envia uma confirmação de recebimento (chamada de *acknowledge* ou *ack*).

Caso essa confirmação não seja recebida, a camada Link de Dados do transmissor reenvia o quadro, já que ele não chegou até o receptor ou então chegou com os dados corrompidos.

3.1.7 CAMADA 1 – FÍSICA

A camada Física pega os quadros enviados pela camada Link de Dados e os transforma em sinais compatíveis com o meio onde deverão ser transmitidos. Se o meio for elétrico, essa camada converte os 0s e 1s dos quadros em sinais elétricos a serem transmitidos pelo cabo. Se o meio for óptico (fibra óptica), essa camada converte os 0s e 1s dos quadros em sinais luminosos e assim por diante, dependendo do meio de transmissão.

Essa camada especifica portanto, a maneira com que os 0s e 1s dos quadros serão enviados para a rede (ou recebidos da rede, no caso da recepção de dados). Ela não sabe o significado dos 0s e 1s que está recebendo ou transmitindo. No caso da recepção de um quadro, a camada Física converte os sinais do cabo em 0s e 1s e envia essas informações para a camada Link de Dados, que montará o quadro e verificará se ele foi recebido corretamente.

O papel dessa camada é efetuado pela placa de rede dos dispositivos conectados em rede. A camada física não inclui o meio onde os dados circulam, somente são necessários os tipos de conectores e cabos de rede usados para transmissão e recepção para que os 0s e 1s sejam convertidos corretamente no tipo de sinal requerido, mas o cabo em si não é responsabilidade da camada.

Existe ainda o padrão de protocolos IEEE 802 em suas versões IEEE 802.3 (*Ethernet*) e IEEE 802.5 (*Token Ring*) com suas camadas Física, Controle de Acesso ao Meio (MAC) e Controle do Link Lógico (LLC). Mas estes não serão neste trabalho abordados.

3.2 NDIS e ODI

Criado pela Microsoft e pela 3Com, o NDIS (*Network Driver Interface Specification*) é um driver instalado no sistema operacional que permite que uma única placa de rede possa utilizar mais de um protocolo de rede ao mesmo tempo. [PERLMAN]

O driver NDIS possui duas partes. A primeira é chamada driver MAC NDIS, que é o driver da placa de rede (que deve ser escrito usando o padrão NDIS).

A segunda parte é chamada *vector*. Essa camada é a responsável por permitir que uma mesma placa de rede possa usar mais de um protocolo, já que o driver da placa de rede (driver MAC NDIS) só permite uma única conexão.

Quando um quadro é recebido pelo driver da placa de rede, ele o passa para a camada *vector*, que o envia para o primeiro protocolo, que poderá aceitar ou rejeitar o pacote. Caso o primeiro protocolo rejeite o quadro, a camada *vector* entrega o quadro ao segundo protocolo. Esse processo continua até que um dos protocolos instalados aceite o quadro ou então todos o tenham rejeitado.

Outra finalidade da especificação NDIS é possibilitar a existência de mais de uma placa de rede em um mesmo micro. Muitas vezes esse procedimento é necessário para ligar um mesmo micro a dois segmentos de rede diferentes. [MICROSOFT]

Em princípio, sem o NDIS, com duas placas de rede em um mesmo micro seriam necessárias duas pilhas de protocolos completas, uma para cada placa de rede (isto é, seguindo o modelo OSI seriam necessários protocolos completos com sete camadas para cada placa de rede instalada). Com o NDIS, uma única pilha de protocolos é compartilhada (isto é, as camadas 4, 5, 6 e 7 do modelo OSI) com todas as placas de rede instaladas, já que o que existir acima da camada *vector* poderá ser compartilhado por todas as placas de rede.

O ODI (*Open Datalink Interface*) é um driver com o mesmo objetivo que o NDIS, criado pela Novell e pela Apple para os seus sistemas operacionais, mas com um funcionamento um pouco mais complexo e mais completo. A grande diferença entre o NDIS e o ODI é o uso da camada Controle de Link Lógico (LLC) que não é usada no NDIS. No NDIS há a camada *vector*, que possui funcionamento similar, porém funciona de maneira diferente. No modelo ODI essa camada é chamada Camada de Suporte ao Link (*Link Support Layer*).

Neste modelo são adicionadas duas interfaces, uma chamada interface para Múltiplos Protocolos (MPI – *Multi Protocol Interface*), que faz a interface entre a Camada de Suporte ao Link e os drivers das placas de rede instaladas. Os drivers da placa de rede compatíveis com o padrão ODI são chamados MLID ou *Multiple Link Interface Driver*. [INTEL]

A principal diferença entre o NDIS e o ODI é que, como a camada de Controle do Link Lógico ou Camada de Suporte ao Link, como chamada no ODI, possui um campo de endereçamento de protocolos, tanto o transmissor quanto o receptor sabem qual é o protocolo que está sendo usado no dado que foi encapsulado dentro do quadro.

Com isso, ao receber um quadro, a interface de múltiplos protocolos (MPI) entrega diretamente os dados para o protocolo responsável. No NDIS, quando um quadro chega, a camada *vector* tenta encaminhar o quadro para cada um dos protocolos instalados, até um deles aceitar (ou todos rejeitarem), já que não há o campo do endereçamento.

A existência da Interface para Múltiplos Links (MLI) permite a instalação de mais de uma placa de rede na máquina, tendo as vantagens que já foram explicadas no NDIS, isto é, as duas placas de rede podem compartilhar os protocolos existentes acima desta camada.

O estudo aqui desenvolvido é de fundamental importância, pois é primeiramente necessário entender como as máquinas se comunicam, qual a linguagem que elas utilizam para que então possa dar início ao desenvolvimento do Software de comunicação livre. Em especial, a camada 5 do modelo OSI de “protocolo ideal”. Existem diversos protocolos, mesmo com todas as diferenças entre eles, mesmo com suas particularidades, todos têm o mesmo objetivo, a transmissão de dados.

4. TCP/IP

O protocolo TCP/IP atualmente é o protocolo mais usado em redes locais. Isso se deve basicamente à popularização da Internet, a rede mundial de computadores, já que esse protocolo foi criado para ser usado na Internet. Mesmo os sistemas operacionais de redes, que no passado só utilizavam o seu protocolo proprietário (como o WindowsNT com seu protocolo NetBEUI e o Netware com o seu IPX/SPX), hoje suportam o protocolo TCP/IP.

Uma das grandes vantagens do TCP/IP em relação a outros protocolos existentes é que ele é roteável, isto é, foi criado pensando em redes grandes e de longa distância, onde pode haver vários caminhos para o dado atingir o computador receptor. [COMER]

Outro fato que tornou o TCP/IP popular é que ele possui arquitetura aberta e qualquer fabricante pode adotar a sua própria versão do TCP/IP em seu sistema operacional, sem a necessidade de direitos autorais a ninguém. [BRISA & EMBRATEL]

Com isso, todos os fabricantes de sistemas operacionais acabaram adotando o TCP/IP, transformando-o em um protocolo universal, possibilitando que todos os sistemas operacionais possam comunicar-se entre si sem dificuldade, o que neste trabalho é de fundamental importância.

A arquitetura do TCP/IP é mostrada na figura 06, onde é feita a correlação das camadas do TCP/IP com as camadas do modelo OSI.[BRISA & EMBRATEL]

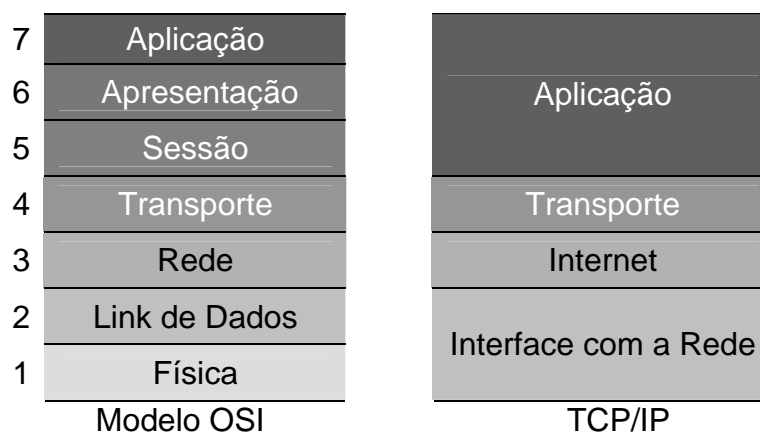


Figura 06 – Arquitetura do TCP/IP

O TCP/IP é, na realidade, um conjunto de protocolos. Os mais conhecidos dão justamente o nome desse conjunto: TCP (*Transmission Control Protocol* – Protocolo de Controle da Transmissão) e IP (*Internet Protocol*), que operam nas camadas Transporte e Internet, respectivamente. [COMER] Mas eles não são os únicos. Serão aqui explicados resumidamente os mais usuais na explicação sobre o funcionamento das camadas do protocolo TCP/IP.

Todos os protocolos do TCP/IP são documentados nos RFCs (*Request for Comments*), que são documentos descritivos do protocolo TCP/IP e que estão disponíveis na Internet. [ALBUQUERQUE]

4.1 CAMADA DE APLICAÇÃO

Esta camada equivale às camadas 5, 6 e 7 do modelo OSI e faz a comunicação entre os aplicativos e o protocolo de transporte. Existem vários protocolos que operam na camada de aplicação. Os mais conhecidos são o http (*HyperText Transfer Protocol*), o FTP (*file Transfer Protocol*), o SNMP (*Simple Network Management Protocol*), o DNS (*Domain Name System*) e o Telnet. [ALBUQUERQUE]

Quando solicitado, cada serviço corresponde a um protocolo específico. No caso de e-mails, este serviço é atendido pelo protocolo SMTP, que, ao ser feita uma solicitação de e-mail (envio ou recebimento) ao TCP/IP, este é atendido pelo SMTP. No caso do www, usado para visualização de páginas, o protocolo usado é o HTTP. Existem ainda inúmeros outros.

A camada de Aplicação comunica-se com a camada de transporte através de uma porta. As portas são numeradas e as aplicações padrões usam sempre uma mesma porta. Por exemplo, o protocolo SMTP utiliza sempre a porta 25, o protocolo HTTP utiliza sempre a porta 80 e o FTP as portas 20 (para transmissão de dados) e 21 (para transmissão de informações de controle).

O uso de um número de porta permite ao protocolo de transporte (tipicamente o TCP) saber qual é o tipo de conteúdo do pacote de dados e, no receptor, saber para qual protocolo de aplicação ele deverá entregar o pacote de dados já que existem inúmeros. [ALBUQUERQUE]

Portanto, ao receber um pacote destinado à porta 25, o protocolo TCP irá entregá-lo ao protocolo que estiver conectado a esta porta, tipicamente o SMTP, que por sua vez entregará o dado à aplicação que o solicitou, o programa de e-mail.

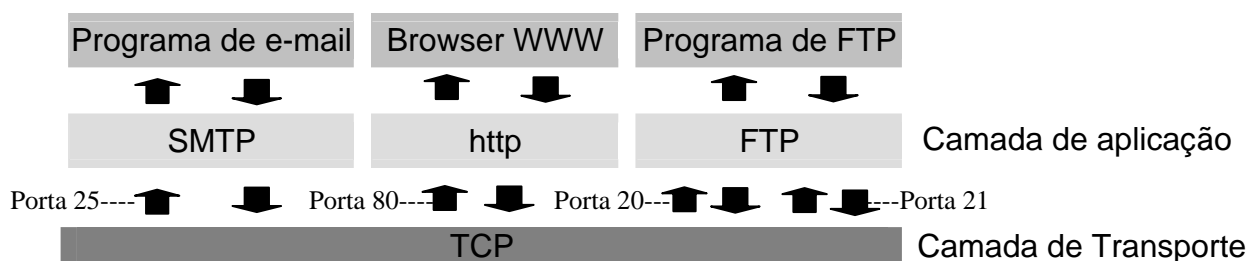


Figura 07– Funcionamento da camada de Aplicação

4.2 CAMADA DE TRANSPORTE

A camada de transporte do TCP/IP é um equivalente direto da camada de transporte (camada 4) do modelo OSI. Esta camada é responsável por pegar os dados enviados pela camada de aplicação e transformá-los em pacotes, a serem repassados para a camada de Internet. [BRISA & EMBRATEL]

No modelo TCP/IP a camada de transporte utiliza um esquema de multiplexação, onde é possível transmitir simultaneamente dados das mais diferentes aplicações. Na verdade, ocorre o conceito de intercalamento de pacotes; [COMER] vários programas poderão estar comunicando-se com a rede ao mesmo tempo, mas os pacotes gerados são enviados à rede de forma intercalada, não sendo preciso terminar um tipo de aplicação de rede para então começar outra.

Isso é possível devido ao uso do conceito de portas, explicado anteriormente, já que dentro do pacote há a informação da porta de origem e de destino do dado. Ou seja, em uma mesma sequência de pacotes recebidos pelo micro receptor, as informações podem não ser da mesma aplicação. Ao receber três pacotes, por exemplo, o primeiro pode ser de e-mail, o segundo de www e o terceiro de FTP.

Nesta camada operam dois protocolos: o já citado TCP (*transmission Control Protocol*) e o UDP (*User Datagram Protocol*). Ao contrário do TCP, este segundo protocolo não verifica se o dado chegou ou não ao destino. [PERLMAN]

Por esse motivo, o protocolo mais usado na transmissão de dados é o TCP, enquanto o UDP é tipicamente usado na transmissão de informações de controle.

Na recepção de dados, a camada de transporte pega os pacotes passados pela camada Internet e trata de colocá-los em ordem e verificar se todos chegaram corretamente. Em redes grandes, especialmente na Internet, os quadros enviados pelo transmissor podem seguir por diversos caminhos até chegar ao receptor. Assim, os quadros podem chegar com erros.

Além disso, o protocolo IP, que é o mais conhecido da camada de Internet, não verifica se o pacote de dados enviado chegou ou não ao seu destino; é o protocolo de transporte (o TCP) que, ao remontar a ordem dos pacotes recebidos, verifica se está faltando algum, pedindo então, a retransmissão daqueles que não chegaram.

4.3 CAMADA DE INTERNET

A camada de Internet do modelo TCP/IP é equivalente à camada 3 (rede) do modelo OSI. [BRISA & EMBRATEL] Assim, todas as explicações dadas sobre essa camada são totalmente válidas para a Camada de Internet do TCP/IP.

São vários os protocolos que podem operar nessa camada: IP (*Internet Protocol*), ICMP (*Internet Control Message Protocol*). ARP (*Addres Resolution Protocol*) e RARP (*Reverse Addres Resolution Protocol*). [COMER]

Na transmissão de um dado de programa, o pacote de dados recebido da camada TCP é dividido em pacotes chamados datagramas.

Os datagramas são enviados para a camada de interface com a rede, onde são transmitidos pelo cabeamento da rede através de quadros. Esta camada não verifica se os datagramas chegaram ao destino, [BRISA & EMBRATEL] isso é feito pelo TCP. Esta camada é responsável pelo roteamento de pacotes, isto é, adiciona ao datagrama informações sobre o caminho que ele deverá percorrer.

4.4 CAMADA DE INTERFACE COM A REDE

Esta camada equivale às camadas 1 e 2 do modelo OSI, é responsável por enviar o datagrama recebido pela camada de Internet em forma de um quadro através da rede. [BRISA & EMBRATEL]

A figura 08 mostra o esquema completo de um computador operando com o protocolo TCP/IP.

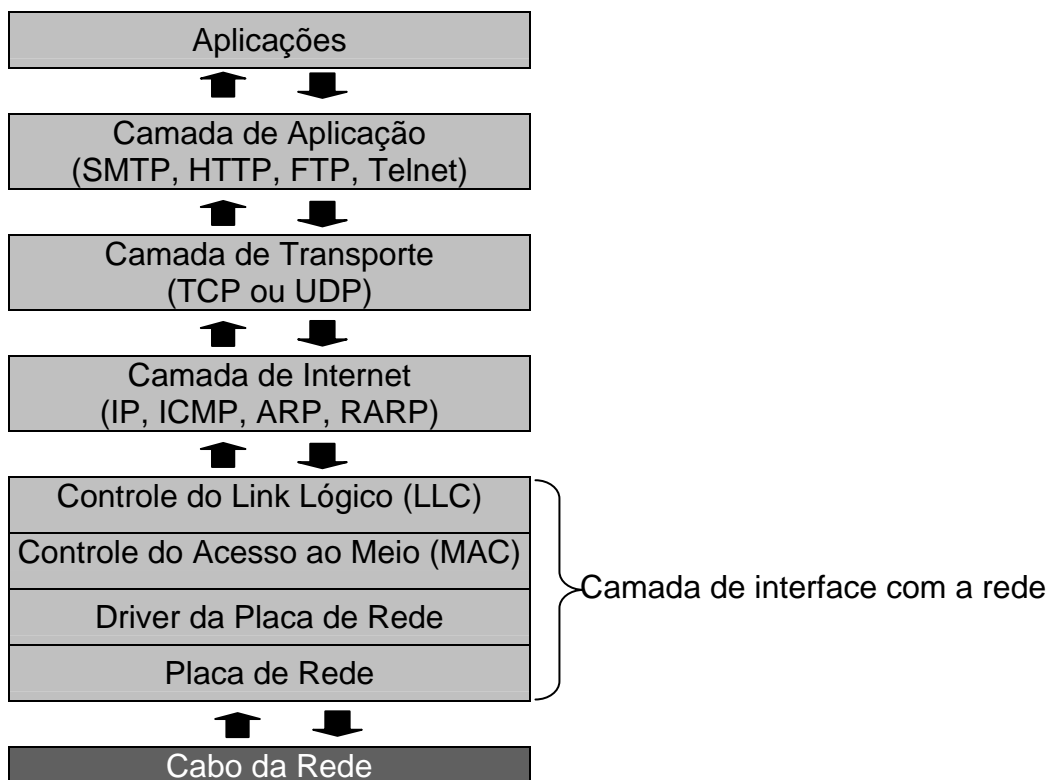


Figura 08– Funcionamento do TCP/IP

O esquema apresentado na figura 08 poderá ter mais uma camada no topo, camada de Interface com a Rede: NDIS ou ODI, já mencionados anteriormente, caso o sistema operacional use algum desses padrões.

Como apresentado no início do capítulo, esse protocolo tem um destaque no estudo por ser o protocolo escolhido. Utilizando o TCP/IP podemos ter o acesso por vários meios, seja via telefone *Dial Up*, seja via rede, seja pela Internet, enfim, temos uma gama enorme de possibilidades. Como visto no capítulo 2, o Software de Comunicação utilizado opera com os protocolos proprietários NetBEUI da Microsoft e com o IPX/SPX da Novell. Além de proprietários, estes não são tão completos quanto ao TCP/IP, reforçando assim a escolha deste.

5. APLICAÇÃO E DISCUSSÃO

5.1 WAKE UP ON RING (WOR)

Esse recurso permite que computadores sejam ligados e desligados remotamente através da linha telefônica. Assim, o usuário pode ligar, acessar e desligar um computador que esteja localizado a quilômetros dele. Para esse recurso funcionar, tanto a placa de modem quanto a placa-mãe devem suportá-lo e devemos ligar o modem à placa-mãe através de um cabo com dois fios, em um conector apropriado na placa-mãe (marcado com "*Wake Up On Ring*" ou similar). Além disso, o modem deverá estar ligado à linha telefônica e programado para receber ligações. Um software deverá estar habilitado na máquina para permitir o acesso externo - como o Servidor *Dial Up* do Windows 98 ou como o Software de Comunicação aqui estudado, de modo que o usuário consiga acessar a máquina remotamente (obviamente esse acesso é feito através de um pedido de login e senha). [ATSERVIÇOS]

Assim sendo, o primeiro passo é procurar por dispositivos que suportem esse recurso. Então deve-se observar se a placa mãe escolhida tem suporte para tal. Para saber, basta verificar em seu manual ou verificar fisicamente se possui um conector. A figura 09 a seguir ilustra o referido conector.

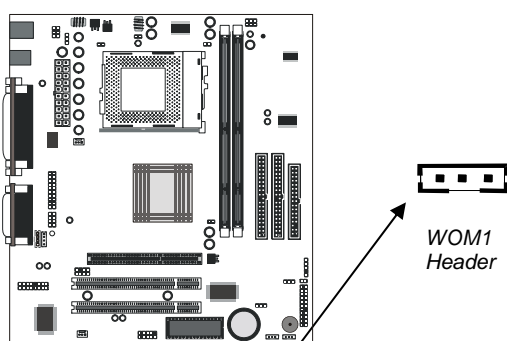


Figura 09 – Conector Wake Up On Modem [PCCHIPS, 2000]

Deve-se também verificar se a placa de comunicação FAX/Modem ou Placa de Rede suporta esse mesmo recurso, tendo essa o mesmo conector existente na placa mãe. No caso da comunicação ser via Modem o referido conector deve ser marcado como *WOM Wake Up on Modem* como ilustrado na Figura 09. Caso a comunicação seja via Rede o conector passa a ser descrito como *WOL Wake Up on LAN*.

Pode-se ainda utilizar uma placa mãe que já possui *Built-in* (integrado) a ela uma controladora de FAX/Modem, neste caso, a grande maioria destas possui o recurso.

Uma vez disponível via hardware, basta agora procurar por um sistema operacional que suporte tal recurso bem como um software para comunicação.

No exemplo aqui descrito, faz-se uso do sistema operacional Microsoft WindowsXP e do software para comunicação Symantec pcAnywhere, o qual é descrito no capítulo 2. Porém, deve-se lembrar que estes são Softwares Proprietários, de custo elevado, podendo utilizar uma plataforma livre e desenvolver um Software livre para esta plataforma. As vantagens de operabilidade e de compatibilidade com todos os itens de *Hardware* forma fundamentais na escolha deste Sistema Operacional e deste Software de Comunicação. Poderiam-se utilizar Sistema Operacional e Software de Comunicação livres, porém sem os resultados desejados.

Usaram-se então 2 microcomputadores para teste. O primeiro deles um microcomputador INTEL PentiumIII com placa mãe ASUS P3B-F e placa de comunicação FAX/Modem IBM AT&T (os quais suportam o recurso) utilizado como *Host* que receberia a ligação. O segundo é um microcomputador INTEL PentiumIII com placa Mãe PCChips M756, a qual possui a controladora de comunicação integrada utilizado como o Controlador Remoto, o microcomputador que liga para o *Host*.

O primeiro passo foi a configuração da BIOS da placa mãe do micro *Host*, habilitando e configurando o recurso *Wake Up on Modem Ring* via *setup*. Uma vez feito isso, foi necessário então configurar a plataforma e o Software de Comunicação.

Para a troca de dados, foi então configurado o software pcAnywhere, para se ter um maior acesso, com uma maior segurança.

Serão agora ilustrados mais especificamente os equipamentos e softwares utilizados.

5.2 PLACA MÃE ASUS P3B-F

Conforme descrito anteriormente, na escolha da placa mãe do microcomputador deve-se verificar se a mesma possui suporte ao recurso aqui estudado. Isso é feito, primeiramente conferindo seu manual, conforme apresentado nas figuras a seguir.

ASUS		Motherboard P3B-F	
JumperFree™ BIOS	Allows processor settings and easy overclocking of frequency and Vcore voltages all through BIOS setup when JumperFree™ mode is enabled. Easy-to-use DIP switches instead of jumpers are provided to manually setup the processor.	AGP Slot	Supports an Accelerated Graphics Port card for high performance, component level interconnect targeted 3D graphical display applications using a 1X or 2X mode bus.
Smart BIOS	2Mb firmware provides Vcore and CPU/SDRAM frequency adjustments, boot block write protection, and HD/SCSI/MD/ZIP/CD/Floppy boot selection. Power supply is auto- detected to enable/disable Suspend-To-RAM and KB / PS/2 mouse power up, eliminating the need to make jumper adjustments.	SMBus	Features the System Management Bus interface, which is used to physically transport commands and information between SMBus devices.
Multi - device Wake Up	Supports modem wake up, keyboard / PS/2 mouse wake up, and LAN card wake up functions from sleep or soft-off mode.	PCI & ISA Expansion Slots	Provides options of five 32-bit PCI (rev 2.2) with two 16-bit ISA expansion slots, six PCI with one ISA, and six PCI with no ISA *. All PCI slots can support Bus Master PCI cards, such as SCSI or LAN cards. (PCI supports up to 133MB/s maximum throughput.)
PC Health Monitoring	Provides an easier way to examine and manage system status information such as CPU and system voltages, temperatures, and fan status through the onboard hardware ASIC and the bundled LDCM from Intel® or PC Probe from Asus.	Multi - I/O	Provides two high-speed UART compatible serial ports and one parallel port with EPP and ECP capabilities. UART2 can also be directed from COM2 to the Infrared Module for wireless connections.
Enhanced ACPI & Anti - Boot Virus Protection	Programmable BIOS (flash EEPROM), offering enhanced ACPI for Windows 98 compatibility, built-in firmware-based virus protection, and auto-detection of most devices for virtually automatic setup.	Ultra DMA/33 Bus Master IDE	Comes with an onboard PCI Bus Master IDE controller with two connectors that support four IDE devices in two channels. Supports UltraDMA/33, PIO Modes 3 and 4, and Bus Master IDE DMA Mode 2, as well as Enhanced IDE devices, such as Tape Backup, CD-ROM, CD-R/W, and LS-120 drives.
		Universal Retention Mechanism	Supports a Pentium® III / II processor packaged in a Single Edge Contact Cartridge (SECC2/SECC) or a Celeron™ processor packaged in a Single Edge Processor Package (SEPP).

Figura 10 – Manual placa mãe ASUS [ASUS, 2000]

Consultando o manual pode-se conferir que esta placa mãe tem suporte ao recurso (em destaque na figura 10). Mas as informações aqui contidas ainda não são suficientes, precisando conferir de maneira mais detalhada. Avançando a consulta do referido manual pode-se então constatar que é afirmativa a resposta, esta placa mãe suporta o recurso *Wake up on ring e Wake on LAN*, pois tem os conectores necessários, conforme destacado na figura 11.

ASUS		Motherboard P3B-F	
Wake - On - LAN	Supports Wake-On-LAN activity through an optional ASUS PCI-L101 10/100 Fast Ethernet PCI card or a similar ethernet card.	Suspend and Go!	Suspend-to-RAM (STR) provides maximum power savings (average of 5 watts) as an alternative to leaving the computer ON and QuickStart™ so that you do not fall asleep waiting for system bootup (Suspend-to-RAM requires OS support and does not support ISA cards; ISA cards may fail to work coming out of STR mode).
Wake - On - Ring Connector	Supports Wake-On-Ring activity through a PCI modem card which supports a WQR connector.	Easy Installation	Incorporates BIOS that supports auto-detection of hard disk drives, PS/2 mouse, and Plug and Play devices to make the setup of hard disk drives, expansion cards, and other devices virtually automatic.
IrDA	Supports an optional infrared port module for a wireless interface.	PC' 99 Compliant	Both the BIOS and hardware levels of ASUS motherboards meet PC' 99 compliancy. The new PC' 99 requirements for systems and components are based on the following high-level goals: Support for Plug and Play compatibility and power management for configuring and managing all system components, and 32-bit device drivers and installation procedures for Windows 95/98/NT. Color-coded connectors and descriptive icons make identification easy as required by PC' 99.
Onboard LED	The onboard LED will light up when there is standby power to the PCI bus. This acts as a reminder to the user to turn OFF the power before plugging and unplugging devices so as not to damage the motherboard, peripherals, and/or components.	Symbios SCSI BIOS	Supports optional ASUS SCSI controller cards through the onboard SYMBIOS firmware.
Desktop Management Interface (DMI)	Supports DMI through BIOS, which allows hardware to communicate within a standard protocol creating a higher level of compatibility. (Requires DMI-enabled components.)	Concurrent PCI	This allows multiple PCI transfers from PCI master buses to the memory and processor.
ACPI Ready	Advanced Configuration Power Interface (ACPI) provides more Energy Saving Features for operating systems that support OS Direct Power Management (OSPM) functionality. With these features implemented in the OS, PCs can be ready around the clock, yet satisfy all the energy saving standards. To fully utilize the benefits of ACPI, an ACPI-supported OS such as Windows 98 must be used.		

Figura 11 – Manual placa mãe ASUS [ASUS, 2000]

Agora que já se sabe que fisicamente esta placa mãe suporta o recurso, precisa-se saber então se sua BIOS (*Basic Input Output Settings*) permite a utilização do mesmo. Consultando a BIOS, na guia de gerenciamento de energia, pode-se então obter a resposta afirmativa. Habilita-se então o recurso e se dá início ao uso do mesmo.

AMIBIOS SETUP – POWER MANAGEMENT SETUP	
<C>1998 American Megatrends, Inc. All Rights Reserved	
Power Management/APM	Disabled
Standby Time Out <Minute>	Disabled
Suspend Time Out <Minute>	Disabled
Hot Key Power On	Disabled
Ring On Power On	Disabled
RTC Alarm Power On	Disabled
RTC Alarm Date	15
RTC Alarm Hour	12
RTC Alarm Minute	30
RTC Alarm Second	30
ESC : Quit ↑↓↔ : Select Item F1 : Help PU/PD/+/- : Modify F5 : Old Values <Shift>F2 : Color F6 : Load BIOS Defaults F7 : Load Setup Defaults	

Figura 12 – BIOS [PCCHIPS, 2000]

Pode-se conferir no mesmo manual, conforme figura 13, que traz inclusive uma breve descrição do recurso que todo o conjunto oferece suporte, restando agora apenas fazer uso dos mesmos, instalando e configurando-os.

ASUS		Motherboard P3B-F	
Temperature Monitoring and Alert	To prevent system overhear and system damage, this motherboard supports processor thermal sensing and auto-protection.	Double the IDE Transfer Speed	ASUS smart series motherboards with Intel® chipsets improves IDE transfer rate using Bus Master UltraDMA/33 IDE which can handle data transfer up to 33MB/s.
Voltage Monitoring and Alert	System voltage levels are monitored to ensure stable current to critical motherboard components. Voltage specifications are more critical for future processors, so monitoring is necessary to ensure proper system configuration and management.	SDRAM Optimized Performance	Supports the new generation memory - Synchronous Dynamic Random Access Memory (SDRAM) which increases the data transfer rate to 800MB/s max using PC100-compliant SDRAM.
System Resources Alert	Today's operating systems such as Windows 98, Windows NT, and OS/2, require much more memory and hard drive space to present enormous user interfaces and run large applications. The system resource monitor will warn the user before the system resources are used up to prevent possible application crashes. Suggestions will give the user information on managing their limited resources more efficiently.	Auto Fan Off	The system fans will power off automatically even in sleep mode. This function reduces both energy consumption and system noise, and is an important feature in implementing silent PC systems.
Dual Function Power Button	Through BIOS, the power button can be defined as the "Stand by" button or as the Soft-Off button. Regardless of the setting, pushing the power button for more than 4 seconds will enter the Soft-Off mode.	Dual Function Power Button	Pushing the power button for less than 4 seconds when the system is in the working state places the system into one of two states: sleep mode or soft-off mode, depending on the BIOS or OS setting. When the power button is pressed for more than 4 seconds, the system enters the soft-off mode regardless of the BIOS setting.
Remote Ring On (requires modem)	This allows a computer to be turned on remotely through an internal or external modem. With this benefit on-hand, users can access any information from their computers from anywhere in the world.	Fan Status Monitoring and Alarm	To prevent system overhear and system damage, the CPU, power supply, and system fans can be monitored for RPM and failure. All fans are set for its normal RPM range and alarm thresholds.
Message LED (requires ACPI OS Support)	Message LEDs now act as information providers. Through the way a particular LED illuminates, the user can determine the stage the computer is in. A simple glimpse provides useful information to the user.	PS/2 Keyboard/Mouse Power Up	Keyboard/Mouse Power Up can be enabled or disabled to allow the computer to be powered on by pressing the space bar on the keyboard or moving the mouse.

Figura 13 – Manual placa mãe ASUS [ASUS, 2000]

5.3 PLACA MÃE PCCHIPS M756LMRT+

A configuração da segunda placa mãe representou uma tarefa mais simples, se comparada a anterior, primeiramente por esta ser apenas o micro controlador dispensando a utilização do recurso *Wake Up* e posteriormente por esta possuir suporte ao recurso aqui estudado, mas com uma vantagem, as placas controladoras de comunicação, FAX/Modem e Rede, já estão integradas (*On Board*), dispensando assim a preocupação em encontrar uma controladora de comunicação. Consultando o manual, pode-se ainda encontrar uma breve explicação do recurso e de como configura-lo, mesmo não sendo necessário seu uso, facilitando assim o trabalho.

A figura14 ilustra uma breve descrição da referida placa.



M756LMRT+



The advanced features of the PC133 GFXCEL System Board include :

- Supports Pentium III 450~866MHz, FC-PGA Pentium III 500M~1.13GHz, Pentium II 233~550MHz and Celeron 266~766MHz CPUs with frequency at 66/100/133MHz in Slot 1/Socket 370 for MicroATX Form Factor.
- Provides 2 DIMMs for PC133 SDRAM modules, and memory size is expand up to 1GB.
- Highest performance, 128-bit 3D AGP Graphics Accelerator with 64MB (max.) frame buffer embedded in North bridge; up to 1920x1200 16M resolutions, AGP V2.0 Spec. Complies.
- 3D PCI Sound Pro on board, meets PC98 Spec., HRTF Positional Audio supports Microsoft's Direct Sound 3D and Aureal's A3D compatible interface, with 4 channel speaker out ; Software Wave-table Synthesizer.
- 10/100Mbps Fast Ethernet LAN on board, supports IEEE 802.3 and 802.3u standards, and fully compliant ANSI X3.263 TP-PMD physical sub-layer (optional).
- 56K Fax/Modem on board, supports V.90 Fax/Modem standard for internet communication.
- 2MB Flash ROM on board, provides complete Advance Configuration Power Interface (ACPI) and Legacy PMU; Ultra DMA 66; fully compliant with PC97 and PC98 Spec.
- Provides ATX power connector supports various functions of ATX Power such as Suspend, Shutdown, Wake on LAN, Wake on Modem, Wake on Alarm, Interrupt Wake-Up from Keyboard/Mouse, and Keyboard Power On/Off.
- Built-in Hardware Monitor circuit supports thermal, power and fan speed monitor.
- Supports both Slot 1 and Socket 370 Processors for flexible CPU selection.
- Supports PC 99 Color Connector for easy identification of peripheral devices.
- Optional extended USB card for extra USB ports connection.
- Bundled Corel WordPerfect Suite 8; take advantage of leading-edge collaboration and business tools (optional).
- Bundled 3Deep, to deliver the precise imagery and display accurate color in your monitor.
- Bundled Gamut 2000 includes MP3 Encoder/Decoder, for proceffessional audio applications.
- Bundled Super Voice for Fax/Modem and Voice application; MediaRing Talk for Internet Phone communications.
- Provides Trend Micro's ChipAwayVirus and PC-Cillin 98 (OEM) for Windows 95/98 and internet virus protection.

Figura 14 – Descrição placa mãe PCChips M756LMRT+ [PCCHIPS, 2000]

Como visto na Figura 14, esta placa mãe também suporta o recurso aqui estudado, mas nos alerta de um detalhe, a alimentação da placa deve ser padrão ATX para que o computador possa permanecer em *Stand By* ou “dormindo”. Caso a alimentação seja por algum outro padrão, todo o recurso aqui estudado se torna nulo. Esse é um detalhe muito importante a ser lembrado na escolha dos itens de Hardware, o gerenciamento de energia.

5.4 PLACA DE COMUNICAÇÃO IBM AT&T

Esta é a placa controladora de comunicação FAX/Modem escolhida para ser utilizada no microcomputador *Host* do estudo aqui apresentado por ser compatível e por suportar o recurso. Seu padrão de barramento é ISA com velocidade de comunicação 33.6Kilobits por segundo. Esta placa possui o conector *Wake Up on Modem Ring* e o cabo para então ligar à placa mãe.

5.5 INSTALAÇÃO E CONFIGURAÇÃO

Uma vez instalados os equipamentos, configura-se a BIOS do equipamento para que na opção *Ring On Power On*, conforme descrito na Figura 12, seja então habilitado o recurso.

Uma vez configurada a BIOS, deve-se então instalar os *drivers* do dispositivo de comunicação FAX/Modem ou Rede no sistema operacional. No estudo aqui desenvolvido opto-se pelo FAX/Modem. O Sistema Operacional escolhido, Microsoft WindowsXP já possui os referidos *drivers* integrados a ele, dispensando assim a instalação via meios externos. O que contribui ainda mais para escolha deste Sistema Operacional, pois em uma plataforma livre, seria necessária a instalação via meios externos, como descrito.

Uma vez concluído o processo de instalação dos dispositivos de Hardware, dá-se início então ao processo de instalação e configuração do Software de comunicação. Cabe salientar que o equipamento escolhido deve apresentar previamente a plataforma e o Sistema Operacional – com o software de comunicação escolhido – devidamente instalados e configurados.

Como descrito anteriormente, o Software aqui utilizado foi o Symantec pcAnywhere. Este funciona nas plataformas Novell e Microsoft Windows, em todas as suas versões. Optamos pela plataforma Microsoft Windows, já previamente instalada e configurada em ambos os equipamentos, o *Host* e o controlador remoto.

5.4.1 INSTALAÇÃO E CONFIGURAÇÃO DO SOFTWARE

Uma vez escolhido e devidamente adquirido o Software de Comunicação, o usuário passa então a usufruir de uma ferramenta muito útil, com muitos recursos e com muitas vantagens, como descrito neste subcapítulo. Como já dito, o Software escolhido foi o Symantec pcAnywhere. Dá-se então início ao processo de instalação de maneira muito rápida e simples, pois o CD de instalação é auto-executável, onde, ao inserir o CD no *drive* o mesmo já dá início ao processo de instalação na sua tela inicial, conforme ilustrado na Figura 15.

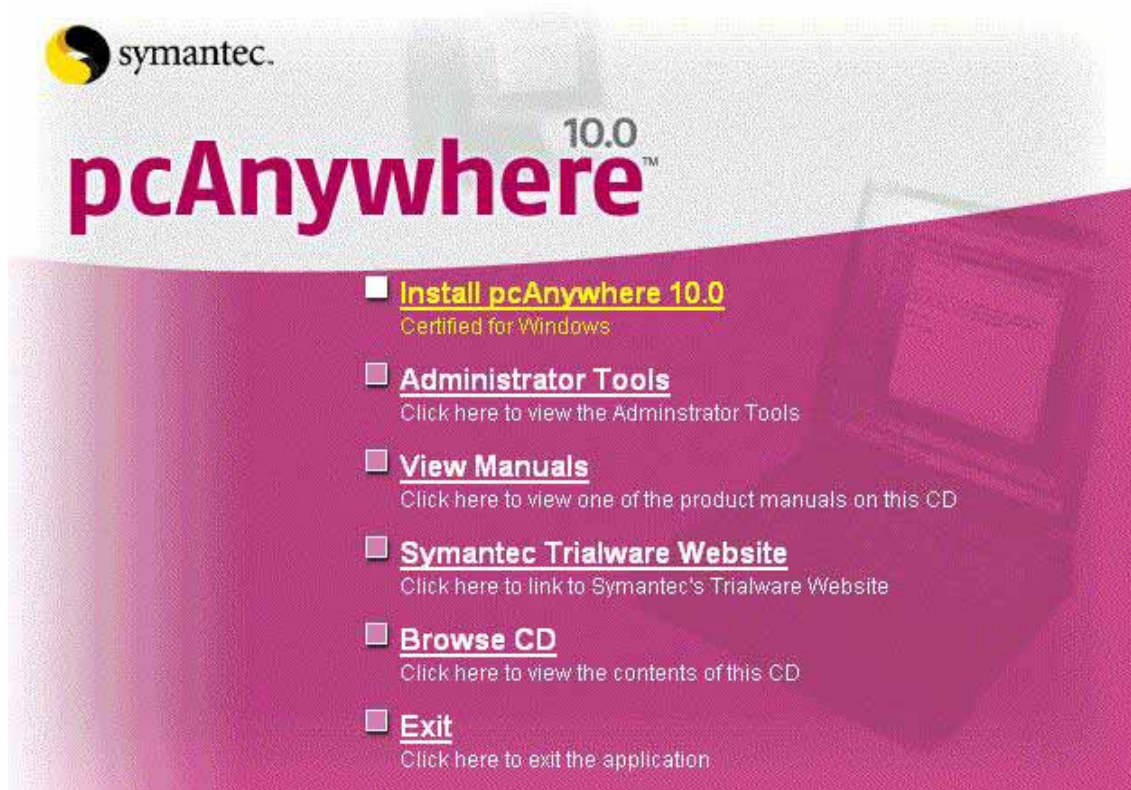


Figura 15 – Tela inicial do Symantec pcAnywhere [SYMANTEC, 2001]

Dentre as características do software quando da sua instalação, destaca-se a sua interface amigável, oferecendo ao usuário opções como, Instalação das ferramentas administrativas, visualização dos manuais, link para o Website do fabricante para o uso de Softwares *Trail* (Cópias de avaliação) e ainda uma ferramenta para visualização do conteúdo do CD e saída.

O primeiro item, *Install* é aqui descrito e ilustrado na Figura 16.

Na tela *Install* o usuário tem as opções de instalação *Professional* que compreende a completude do produto, incluindo o *Packager*, descrito no capítulo 2.4, porém restrito a plataformas Servidor Microsoft Windows NT ou 2000 ou pela opção de instalação *Individual*, que como na *Professional* é o pacote completo, porém sem o recurso *Packager*. Está é a instalação indicada para Windows.

São oferecidas também as opções *Host Only* e *Remote Only* correspondentes aos pacotes de instalação *Remoto* ou *Host* tão somente, sem que sejam instaladas as ferramentas adicionais do pacote completo. Se o usuário escolhe *Remote Only* este poderá apenas trabalhar como Remoto; o Mesmo aplica-se para o pacote *Host Only*.

Existe ainda o pacote *LAN Host*, um pacote pequeno para instalação de *Host* restrito a rede local e a opção de pacote personalizado, onde o próprio usuário cria seu pacote instalação, usando somente os recursos por ele escolhidos.

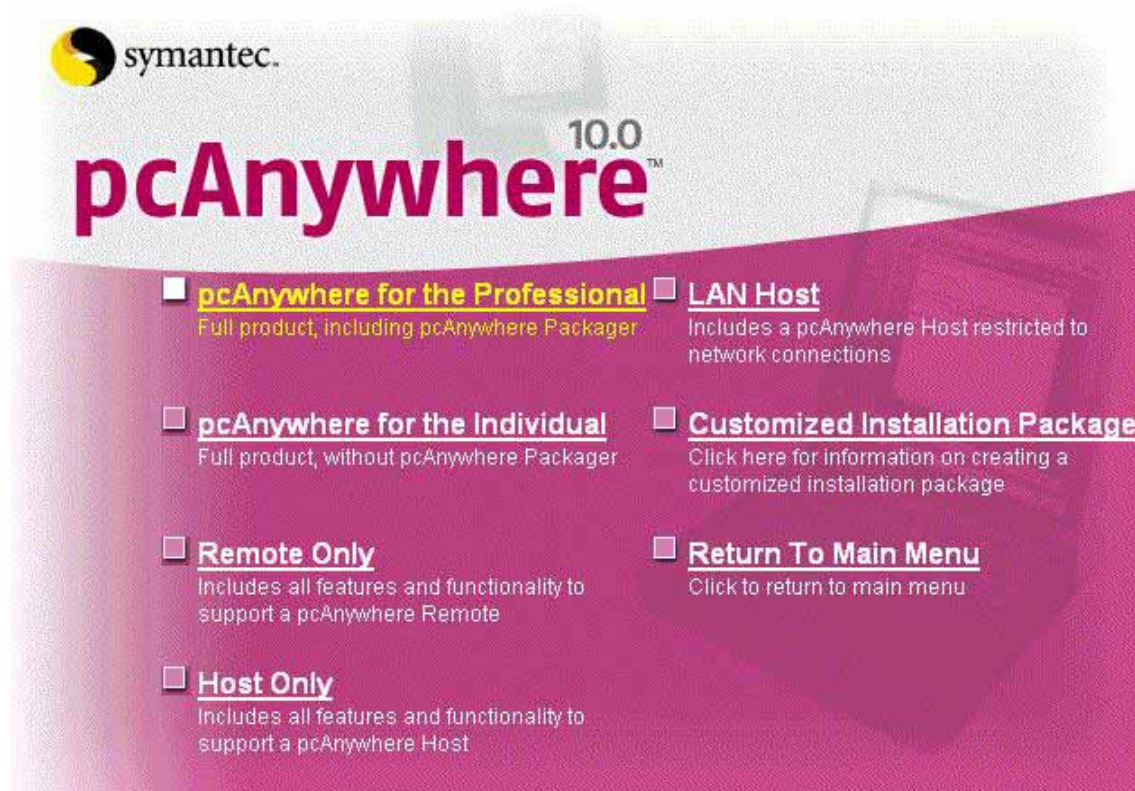


Figura 16 – Tela *Install*. [SYMANTEC, 2001]

No caso específico deste trabalho, optou-se pela instalação *pcAnywhere for the Individual* para o computador que atuará como *Host* pois é completa, não utilizando apenas o *Packager*, uma vez que não se está utilizando uma plataforma Servidor.

Ao clicar sobre o item *pcAnywhere for the Individual* dá-se então início ao processo de instalação.

Ao iniciar a instalação, o Software apresenta um alerta, ilustrado na Figura 17, informando a substituição do MSGINA que controla o *logon* do Windows e conseqüentemente desativará alguns recurso da plataforma WindowsXP como a Troca rápida de usuários, Serviços de terminal e Área de trabalho remota.



Figura 17 – Tela de alerta do pcAnywhere [SYMANTEC, 2001]

Como não difere em nada a utilização de tais recursos, opta-se então pela continuação do processo de instalação do Software.

Em seguida já é apresentada a tela de boas vindas do assistente para instalação, conforme ilustrado na Figura 18.



Figura 18 – Tela de Boas vindas do assistente de instalação [SYMANTEC, 2001]

O assistente descrito na Figura 18 informa que irá instalar o Symantec pcAnywhere no computador. Para continuar é necessário clicar sobre o botão *Next*.

Clicando sobre o botão, a tela seguinte, ilustrada na Figura 19, apresenta o contrato de licença de uso do Software. Essa é uma das principais relevâncias no uso deste Software, seu valor de mercado. É necessário ler o contrato e então dizer se aceita ou não os termos nele contidos para então instalar. Uma vez aceitando, o usuário está sujeito a responder na justiça pelo uso incorreto ou sem o pagamento das licenças ao fabricante. Para aceitar os termos do referido contrato, deve-se selecionar o item *I accept the terms in the licence agreement*, que traduzindo diz: “Eu aceito os termos do contrato de licença de uso”. Selecionado basta então clicar sobre o botão *Next* para a sequência do processo de instalação.

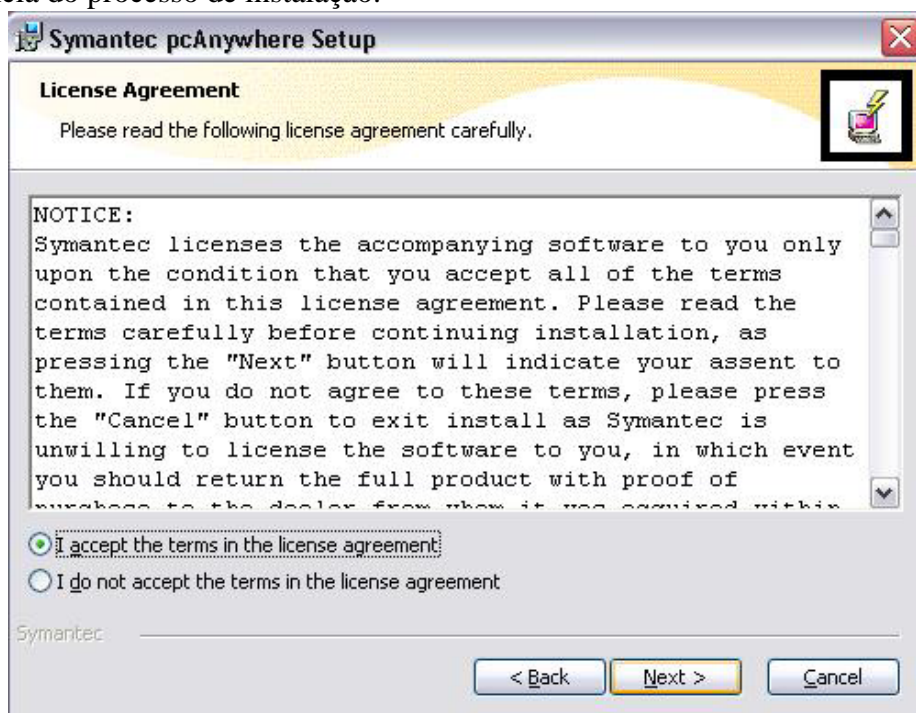


Figura 19 – Contrato de licença de uso do pcAnywhere [SYMANTEC, 2001]

Na tela seguinte, ilustrada na Figura 20, o assistente solicita que usuário informe o seu nome e o nome da empresa compradores do Software. Digitando os respectivos nomes basta então dar continuidade ao processo clicando sobre o botão *Next*.

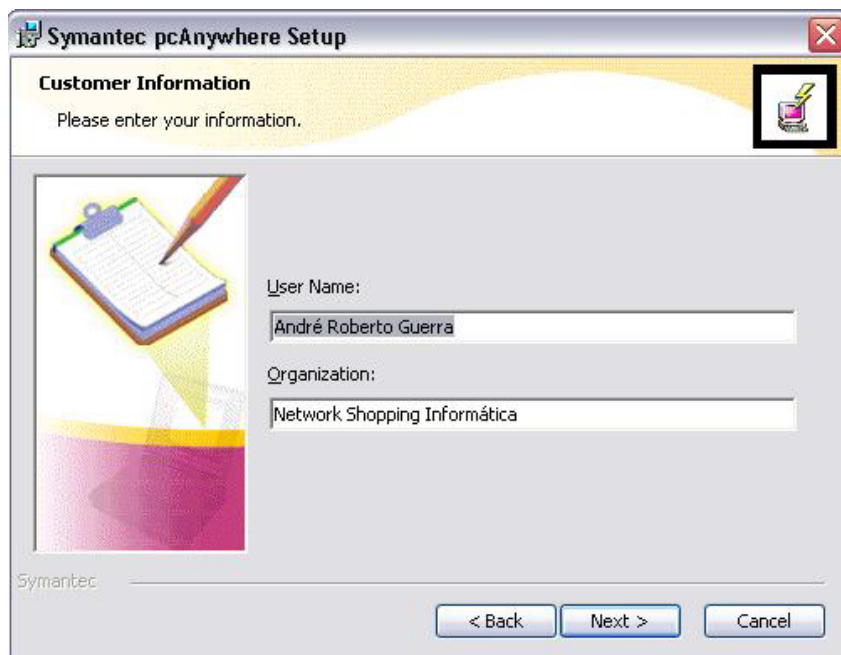
The image shows a screenshot of the 'Symantec pcAnywhere Setup' window. The title bar at the top reads 'Symantec pcAnywhere Setup' with a red close button on the right. Below the title bar, the window has a yellow header area with the text 'Customer Information' and 'Please enter your information.' To the right of this text is a small icon of a computer monitor with a lightning bolt. The main area of the window is light gray. On the left side of this area is a graphic of a clipboard with a pencil and a pink folder. To the right of the graphic are two text input fields. The first is labeled 'User Name:' and contains the text 'André Roberto Guerra'. The second is labeled 'Organization:' and contains the text 'Network Shopping Informática'. At the bottom left of the window is the 'Symantec' logo. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

Figura 20 – Informações sobre o cliente [SYMANTEC, 2001]

Dando seqüência ao processo de instalação, a tela seguinte, ilustrada na Figura 21, solicita ao usuário qual o tipo de instalação que o usuário deseja, se é típica ou customizada. Na instalação típica, recomendada para a grande maioria dos computadores, o Software é instalado com todos os componentes previamente escolhidos na segunda tela e instalado no diretório padrão. Na instalação customizada, o usuário pode alterar tão somente o diretório a ser instalado, pois as opções do Software já foram escolhidas na segunda tela, como dito anteriormente. Essa instalação requer 14MB de espaço em disco. Por conveniência é escolhida a opção de instalação típica, como ilustra a Figura 21.

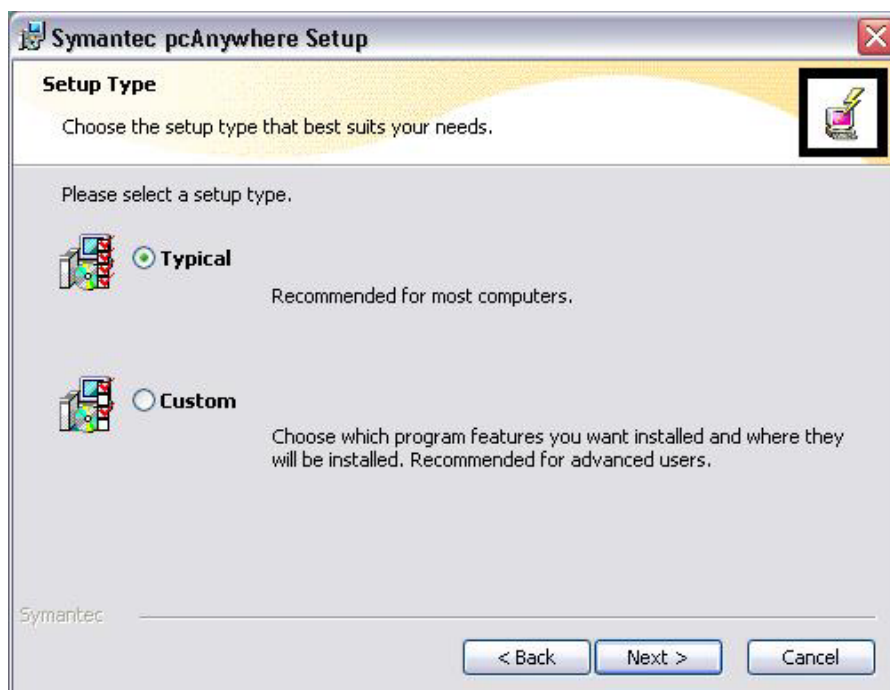


Figura 21 – Tipo de instalação [SYMANTEC, 2001]

Concluídas as etapas, o assistente para instalação já está pronto então para instalar o programa. A tela que nos informa é ilustrada na Figura 22. Para iniciar a cópia dos arquivos basta clicar sobre o botão *Install*.

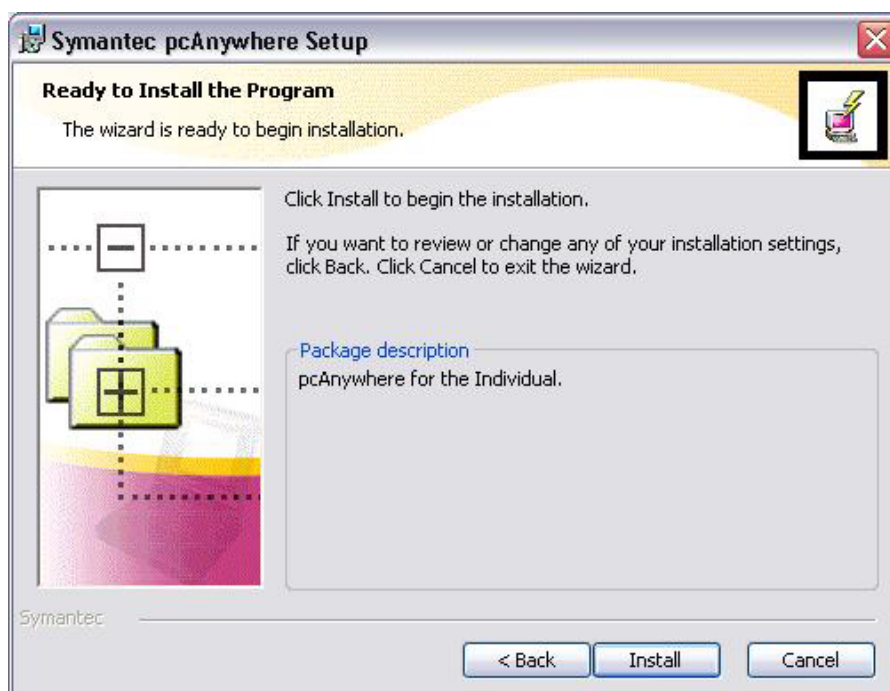


Figura 22 – Tela de início da instalação [SYMANTEC, 2001]

Concluída a instalação, o assistente agora solicita o registro do produto para que se tenha acesso aos recursos que justificam o pagamento do valor da licença de uso. Os serviço de atualização pela internet, ajuda e suporte *on-line*. A Figura 23 ilustra essa tela

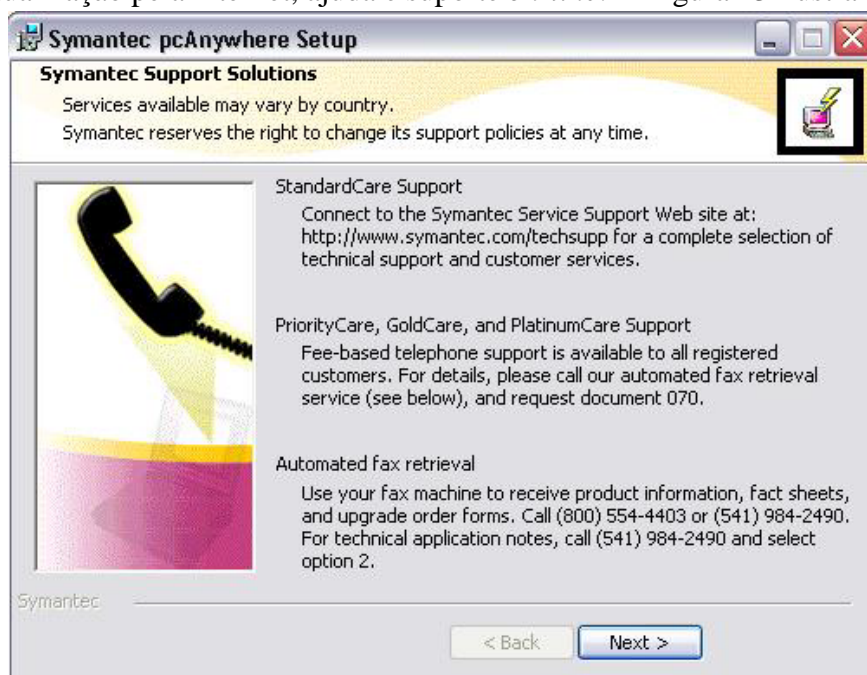


Figura 23 – Soluções de Suporte [SYMANTEC, 2001]

Uma vez registrado, o fabricante já oferece uma atualização do produto pela Internet como ilustra a Figura 24, utilizando a ferramenta LiveUpdate.



Figura 24 – LiveUpdate [SYMANTEC, 2001]

Já instalado e atualizado o Software, o assistente então nos apresenta a tela de conclusão da instalação, como ilustra a Figura 25.



Figura 25 – Conclusão da Instalação. [SYMANTEC, 2001]

Concluída a instalação, o Software solicita a reinicialização do Sistema Operacional para que as alterações tenham efeito. Agora, com tudo pronto, deve-se então configurar o Software para trabalhar como *Host*. Para este processo então deve-se iniciar o Software. Em sua tela principal, ilustrada na Figura 26, ele imediatamente nos apresenta a configuração dos *Hosts*. O Software nos oferece por *Default* a conexão via *Direct Connect* (Conexão Direta via porta de comunicação serial), *Modem* (Conexão via telefone utilizando a porta serial da placa de comunicação e seu respectivo protocolo) e *Network, Cable, DSL* (Conexão via Rede, Internet a Cabo, DSL ou outro tipo de conexão utilizando a placa de Rede). Oferece ainda uma conexão personalizada pelo usuário, onde o próprio usuário determina qual o meio de comunicação e qual protocolo a ser utilizado.

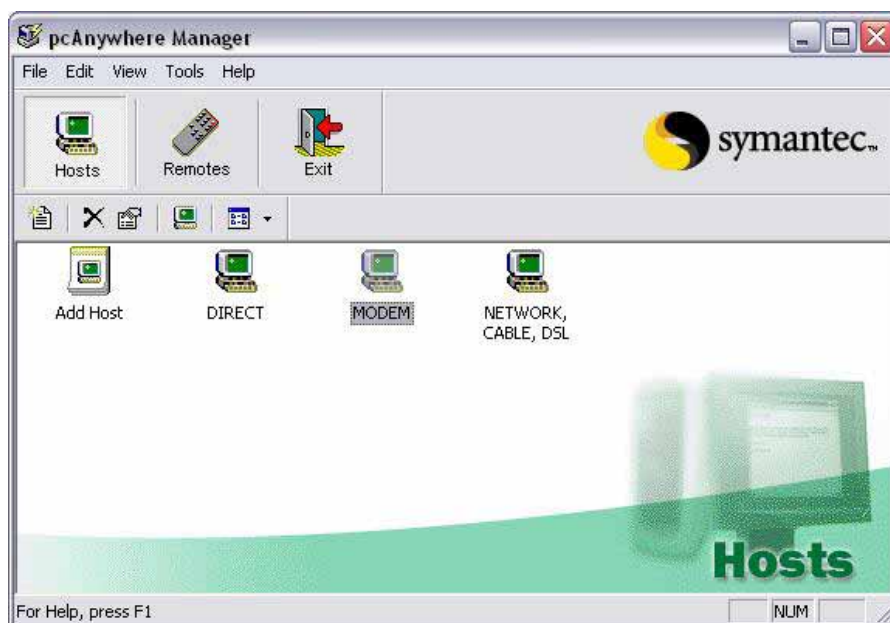


Figura 26 – Tela Inicial do Symantec pcAnywhere [SYMANTEC, 2001]

Como dito anteriormente, os estudos aqui realizados foram desenvolvidos utilizando a conexão via FAX/Modem com o recurso *Wake Up on Modem Ring*. Com isso o *Host* foi devidamente configurado para receber conexões via Modem. Apesar de existir a possibilidade de o usuário criar sua própria conexão, por conveniência optou-se por utilizar a recomendada pelo Software. A configuração da conexão contempla a edição de suas propriedades, onde o usuário fornece as informações necessárias.

Mesmo já sendo oferecida pelo Software, é necessário configurar a conexão. Para isso, basta selecionar a conexão a ser configurada. Após selecionada deve-se editar suas propriedades. Este procedimento é realizado clicando com o botão direito do mouse sobre o ícone da conexão, pressionando as teclas Alt+Enter simultaneamente ou no menu *File/Properties*. Na tela de propriedades do *Host*, sua primeira tela, ilustrada na Figura 27, é a das informações sobre a conexão onde o usuário informa ao software qual a porta de comunicações utilizada pela placa de comunicações (FAX/Modem) e qual o protocolo por ela utilizado. Em nosso exemplo, a porta de comunicações é COM2 e o protocolo escolhido é o TCP/IP.

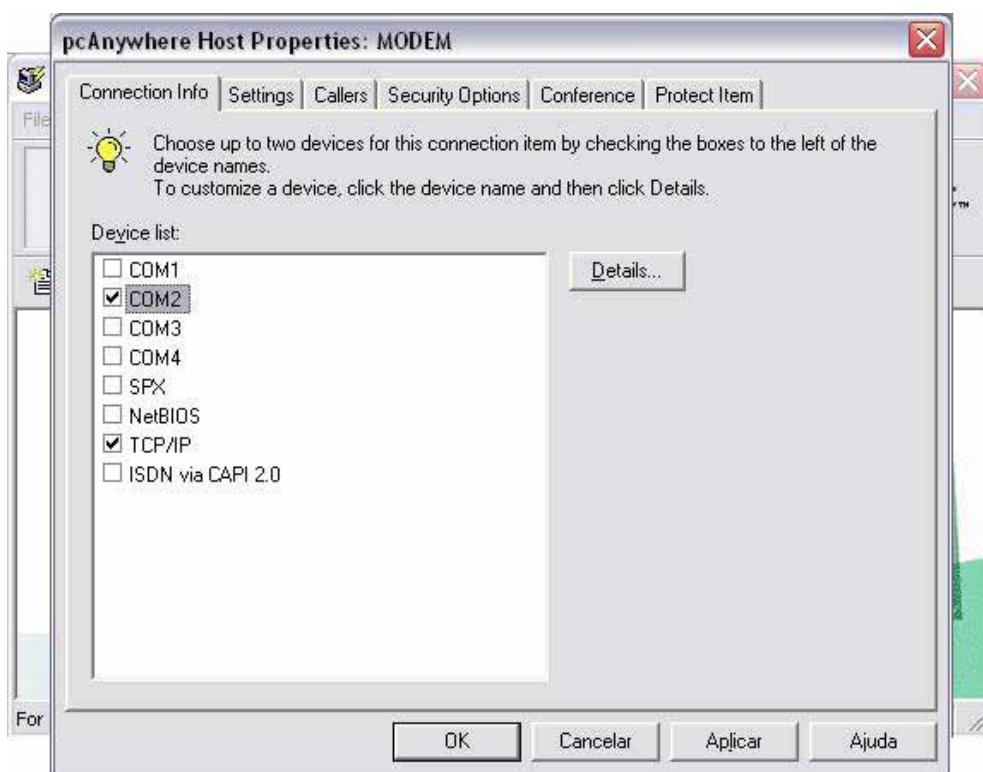


Figura 27 – Propriedades da conexão *Host*. [SYMANTEC, 2001]

Em ambos temos ainda seus detalhes, que seriam suas propriedades adicionais onde é possível determinar a velocidade de conexão da porta utilizada pelo FAX/Modem, a paridade (se existe), o controle de fluxo, como é inicializada e como é encerrada a conexão. Nesta última, uma das maiores vantagens deste Software, é o fato de permitir que a conexão seja iniciada pela indicação de uma chamada telefônica, fazendo assim uso do recurso aqui estudado, como ilustra a Figura 28.

Pode-se ainda verificar que existem outras opções de inicialização e encerramento da conexão.

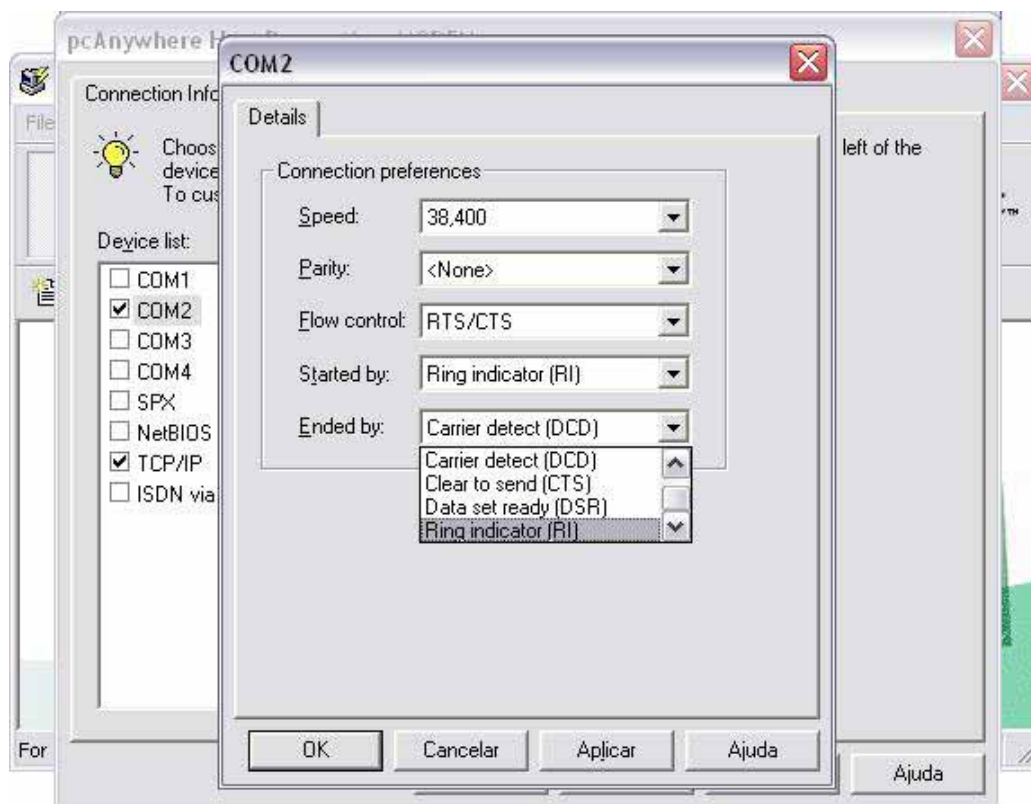


Figura 28 – Preferências do dispositivo de conexão [SYMANTEC, 2001]

Para o protocolo utilizado, TCP/IP, não existem propriedades adicionais, pois o protocolo recebe automaticamente um endereço IP a cada conexão. Para que se tenham propriedades adicionais, é necessário que o *Host* tenha uma conexão estabelecida.

Existe uma segunda guia de propriedades, *Settings*, ilustrada na Figura 29. Nela tem-se as opções de inicialização do *Host*, conexão do Modem, e algumas opções para os finais de conexão normais e anormais. Na inicialização do *Host* pode-se seleccionar a inicialização automática ao Windows ser inicializado, descrita como *Launch with Windows*, pode-se também seleccionar o bloqueio de uma estação Windows NT Workstation, descrita como *Lock NT Workstation*, pode-se ainda seleccionar a execução minimizada no *Tray* do Windows. Descrito como *Run minimized* e a execução como um serviço adicional, descrito como *Run as a service*.

Para a conexão do Modem, o Software oferece uma reconexão, após o tempo determinado pelo usuário em segundos, sem serviço.

Para o final de uma sessão ou conexão anormal, o Software oferece deixar o *Host* aguardando por outro usuário, cancelar o *Host* ou ainda aguardar um tempo, determinando pelo usuário em minutos, para que o mesmo usuário se reconecte.

Todas essas configurações descritas, são ilustradas na Figura 29.

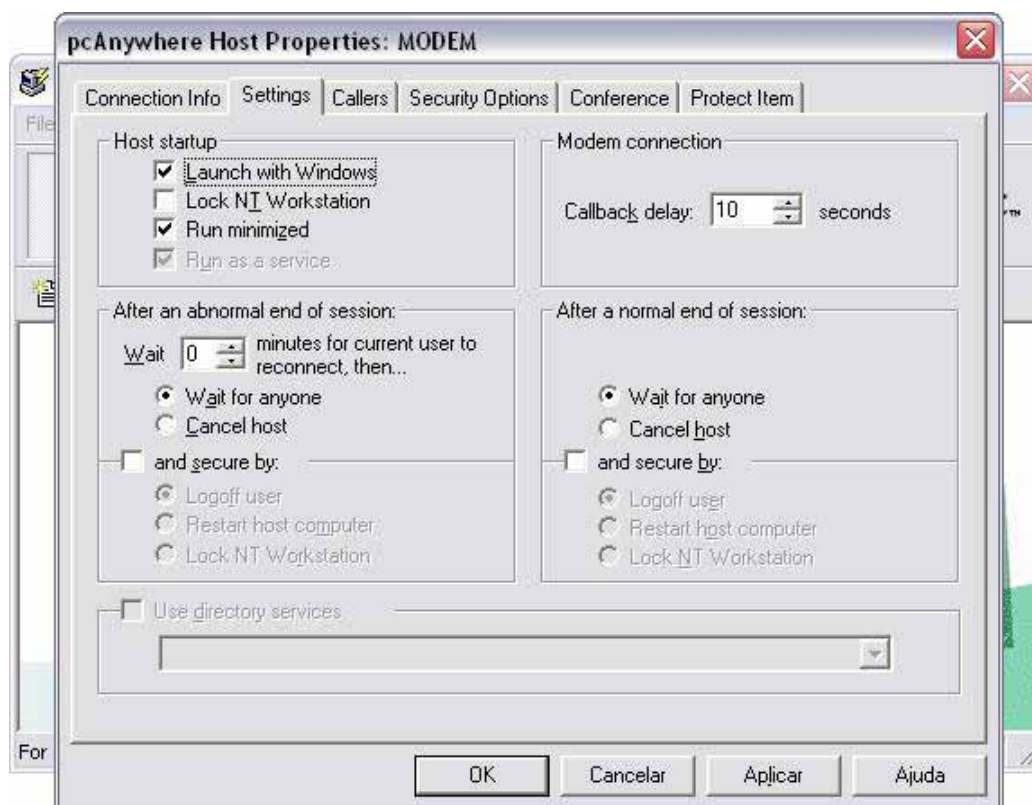


Figura 29 – Configurações adicionais do *Host* [SYMANTEC, 2001]

Na terceira guia, denominada *Callers*, que traduzindo significa “aquele que conecta” ou no Software aqui apresentado o remoto. Nessa guia iremos escolher, dentre os 10 serviços oferecidos, qual o método de autenticação de usuário que será utilizado. Como descrito no capítulo 2, este Software, oferece por *Default* sua própria autenticação, com uma criptografia de 128 bits. Essa tela é ilustrada na Figura 30.

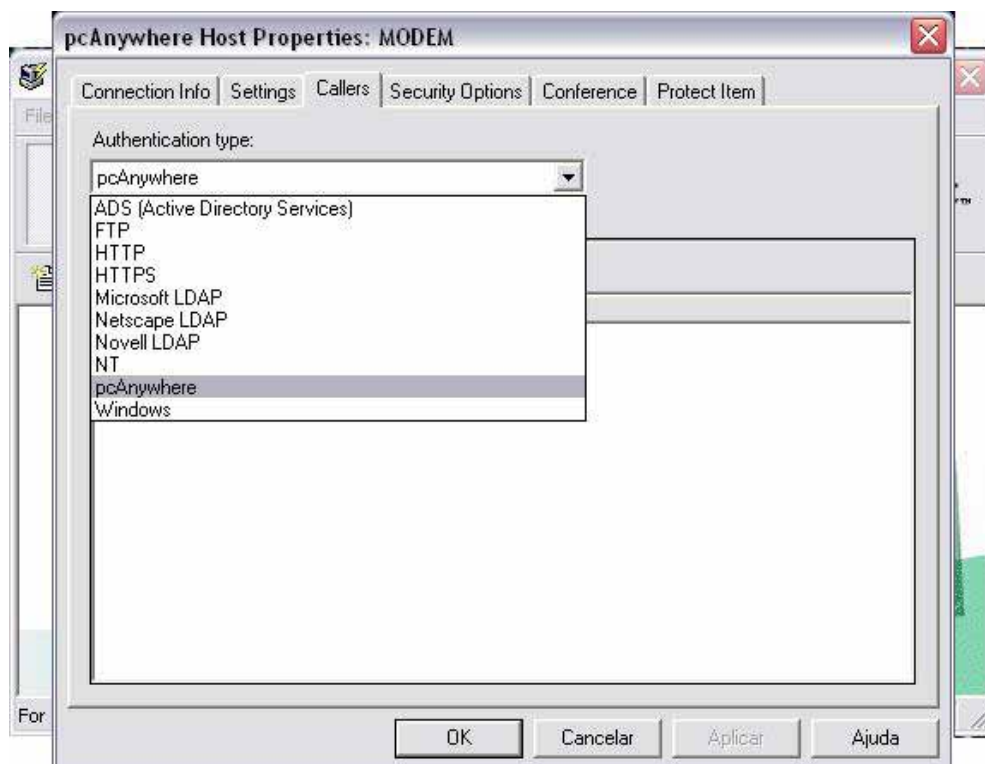


Figura 30 – Configurações adicionais do *Host* [SYMANTEC, 2001]

Escolhido o método de autenticação, no exemplo o escolhido foi o oferecido pelo Software como ilustrado na Figura 30, deve-se então cuidar de adicionar os usuários que poderão então acessar o *Host* e quais os privilégios que os mesmo terão.

Para isso, basta clicar no ícone *New Item* (Novo usuário). Ao clicar é apresentada a tela de propriedades do novo *Caller* (Discador) ilustrada na Figura 31. Na primeira guia, são informados o nome de *Login*, sua senha e confirmação desta senha. Na segunda guia *Callback* o usuário pode então habilitar a função de reconectar em caso de perda da conexão, onde o *Host* liga para um número determinado pelo usuário caso aconteça uma desconexão anormal, como oferecido na tela *Settings* e explicado anteriormente.

Na terceira guia, a mais importante, que é ilustrada na Figura 31, o usuário então configura os privilégios deste *Caller* onde pode-se selecionar entre um *Superuser* que tem permissão de controle total a máquina *Host* ou um *Specify* onde pode-se selecionar o que o usuário pode ou não fazer na máquina *Host*. Especifica-se ainda o tempo limite de conexão e algum comando específico a ser executado automaticamente ao usuário fazer *logon*.

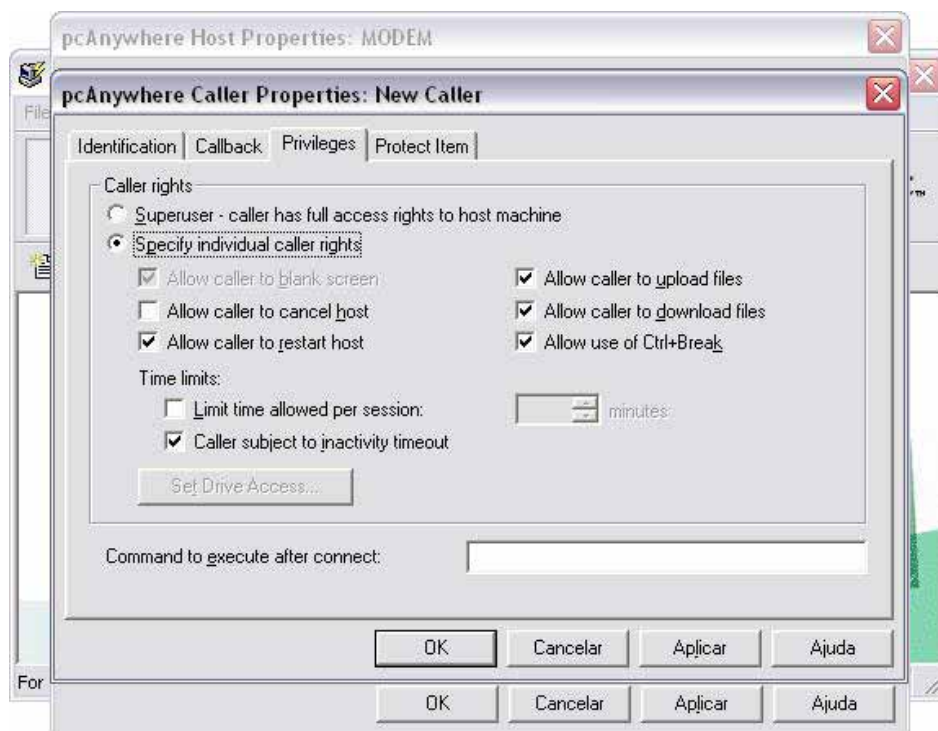


Figura 31 – Privilégios do discador [SYMANTEC, 2001]

Na quarta e última guia de configuração *Callers*, o Software oferece uma proteção extra para a configuração do usuário, uma senha adicional, diferente da senha de usuário para que só o administrador do *Host* possa alterar os privilégios dos usuários da lista.

Na quarta guia de configuração das propriedades do *Host*, *Security Options* (Opções de Segurança), pode-se configurar algumas propriedades adicionais no que tange a segurança, muito bem desenvolvida, onde pode-se selecionar a opção de mostrar um texto de confirmação da conexão com um tempo limite, estabelecido pelo usuário em segundos, e pode-se ainda selecionar a desconexão após esse tempo limite. Pode-se também selecionar a opção de senhas maiúsculas ou minúsculas (*Case Sensitive*), o número de senhas inválidas (*Limit login attempts per call*), o tempo limite para conclusão do *login* (*limit time to complete login*). Pode-se selecionar também quem fica com o controle do teclado e do mouse durante a sessão ou conexão, se o controle é só do *Host*, se é só do remoto ou se é de ambos. Pode-se selecionar a desconexão em caso de inatividade e ainda selecionar a criptografia se usar.

Na quinta guia o Software oferece a opção de conferência, onde o usuário pode estabelecer um endereço IP para conferência.

Oferece também a segurança específica para esta configuração, com uma senha de proteção para esta guia apenas, diferente das outras senhas utilizadas nas outras guias de configuração.

A Figura 32 ilustra essa guia de opções de segurança do *Host*.

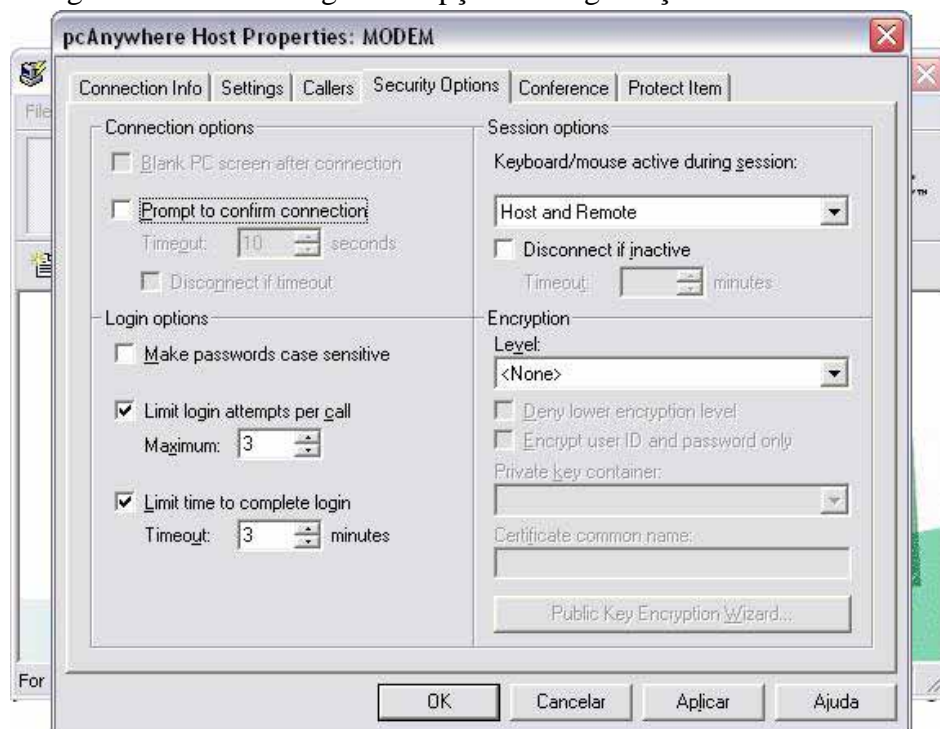


Figura 32 – Opções de segurança do *Host*. [SYMANTEC, 2001]

O Software oferece ainda algumas ferramentas extras, como as opções de configuração do próprio Software, onde o usuário pode habilitar o serviço de gravação de todo o trabalho executado por um remoto no *Host*, pode selecionar o método de apresentação no vídeo, pode selecionar o nome do *Host* como padrão do Windows ou como um nome personalizado. Pode especificar modelos para operação remota, pode selecionar os endereços IP a serem pesquisados, pode configurar o serviço de transferência de arquivos, pode habilitar a gravação de arquivos LOG, serviço de impressão remota, serviço de criptografia, enfim, existem inúmeras opções para a personalização do Software, atendendo assim toda e qualquer necessidade no usuário. Mas tudo com isso com a relevância de ser proprietário e ter um custo elevado.

Para o computador que será usado como remoto, a instalação segue os mesmos passos nesse capítulo descrito, mudando apenas o tipo de instalação, que ao invés de ser completa, passa a ser apenas remoto, um pacote muito menor.

Na versão remoto, o usuário escolherá o meio de comunicação a ser utilizado para o acesso, como no *Host*, criará sua nova conexão ou usará alguma das oferecidas como *default* pelo Software e configurará a mesma para acessar o *Host* desejado.

Tornam-se válidas para o serviço remoto todas as explicações do serviço *Host*, pois o remoto é muito mais simples.

Seguindo os passos aqui descritos, o usuário está apto a trabalhar com o Software aqui apresentado e fazer uso do recurso tema dessa dissertação.

Abre-se então aqui o espaço para estudos futuros, para o desenvolvimento de um Software tão bom quanto o aqui apresentado mas com a vantagem de se livre ou aberto, tornando assim viável a utilização do recurso aqui apresentado.

CONCLUSÃO

Atendendo a proposta inicial deste trabalho, foi desenvolvido um estudo de aplicação que utiliza o recurso *Wake Up*. Como apresentado na introdução deste, não existem bibliografias, não existem referenciais teóricos conceituais, dificultando muito o desenvolvimento destes estudos. Foram necessários meses de pesquisa e estudo em busca de conhecimento, consultando manuais de produtos, em sua grande maioria escritos em língua estrangeira, consultando materiais de cursos extra curriculares de certificação para que se atingisse o ápice no conhecimento deste recurso para conclusão destes estudos.

Com todo o conhecimento adquirido, testaram-se o funcionamento, a implementação e a configuração dos dispositivos de Hardware e Software obtendo o êxito no uso recurso, podendo ligar e desligar um computador à distância, trabalhar com o mesmo, fazendo uso de todos os serviços, de todos os recursos disponíveis, tudo isso de qualquer lugar, trabalhando em seu micro como se estivesse a frente do mesmo, mas com um detalhe de fundamental importância, tudo isso é feito remotamente, não importando quanto distante se encontra.

Um tema de fundamental importância nesse estudo foi a segurança. O Software estudado fornece ótima segurança em todos os níveis, desde a criptografia dos arquivos até a segurança nas configurações do Software. É de fundamental importância, pois uma das principais vantagens desse recurso é o acesso as informações de qualquer lugar, a qualquer hora, mesmo com o equipamento desligado e sem ninguém para ligá-lo. O acesso às informações, cada dia se torna mais importante, e essas informações são cada vez mais valiosas para seus proprietários.

O estudo aqui apresentado serve de referencial teórico conceitual e serve também como uma espécie de manual que ilustra passo a passo cada um dos procedimentos. Com esse material em mãos, qualquer usuários, por mais leigo que seja, é capaz de colocar em funcionamento o recurso e o Software.

Ao final, são propostos aqui estudos futuros. Desde o desenvolvimento de dispositivos com suporte ao recurso até Softwares de comunicação de uso livre, sem custos.

GLOSSÁRIO

ADSL

Asymmetric Digital Subscriber Line, Tecnologia de transmissão de dados em alta velocidade através de linha telefônica comum. No downstream (tráfego de dados na direção do usuário), a ADSL atinge de 1,5 a 9 megabits por segundo (Mbps). E no upstream, as taxas vão de 16 a 640 kilobits/segundo (Kbps). É necessário instalar modems ADSL nas duas pontas.

BIOS

Sigla de *Basic Input/Output System* (Sistema Básico de Entrada/Saída de Dados) também conhecida como o SETUP do computador. Programa carregado em um chip que fica na placa-mãe e gerencia a configuração básica do computador. O BIOS são rotinas que dão instruções para controle dos procedimentos de entrada e saída de dados entre um computador e periféricos e gerenciamento dos dispositivos padrão, como placas de som e vídeo e impressora.

BIT

Binary Digit, unidade básica de um computador. Representa a quantidade mínima de informação que se pode transmitir ou processar

BYTE

Grupo de oito bits e que representa a memória necessária para armazenar um caractere.

CPU

Sigla de *Central Processing Unit* (Unidade Central de Processamento). Trata-se do núcleo e componente principal de um computador, que tem a função de processar e controlar todas as operações executadas. Também chamada de processador.

CRIPTOGRAFIA É a técnica de codificar e decodificar uma mensagem ou mesmo um arquivo utilizando um código secreto. Com o propósito de segurança, das informações nela contidas,

DADO

Termo genérico, utilizado para designar números, letras ou outros caracteres existentes em um computador.

DIAL-UP

Programa usado para acessar outros computadores, através de um modem e de uma linha telefônica. Designação de um tipo de ligação ou de um ato de ligação à Internet, neste caso pelo estabelecimento de uma chamada Dial, para um computador, através de um modem. Método de acesso a uma rede ou computador remoto via rede telefônica, discando o número onde está a rede ou computador

DIGITAL

Representação de dados ou quantidades físicas na forma numérica. Em computadores esses dados são operados pelo sistema binário, um sistema de numeração em que os dígitos são representados apenas pelos números 0 e 1.

DRIVER

Programa que gerencia um dispositivo de entrada e/ou saída de um computador. Exemplos: driver de impressora, de placas de vídeo, de placas de som.

E-MAIL

(CORREIO ELETRÔNICO) Sistema que permite enviar e receber mensagens entre os computadores conectados a uma rede. Uma string que identifica um usuário, permitindo que este usuário possa receber mensagens de correio eletrônico da Internet. Um endereço de correio eletrônico costuma ser formado por um nome que identifica o usuário para o servidor de correio eletrônico, seguido de um sinal de arroba @, do nome do host e do nome de domínio do servidor de correio eletrônico

ETHERNET

Padrão mais popular de redes no qual os computadores são conectados por cabos. Foi desenvolvido pela Xerox. Arquitetura de redes local, baseado na norma IEEE 802.3, que define o método de disputa para redes. Utiliza uma topologia em estrela ou de barramento e se baseia na forma de acesso conhecida como CSMA/CD (Carrier Sense Multiple Access with Collision Detection) para controlar o tráfego nas linhas de comunicação. Os nós da rede são ligados por cabos coaxiais, por cabos de fibra ótica ou por fios de pares trançados.

FIREWALL

Parede de Fogo. É a medida de segurança que pode ser implementada para limitar o acesso de terceiros a um determinada rede ligada à Internet. Os mecanismos de implementação são variados, percorrendo variados tipos de controle por software ou hardware. Um sistema de segurança de rede, cujo principal objetivo é filtrar o acesso a uma rede.

FTP

Sigla de *File Transfer Protocol* (Protocolo de Transferência de Arquivos). Sistema utilizado para transferir arquivos de computadores da Internet para seus usuários e vice-versa.

HARDWARE

Constitui todas as partes físicas, elétricas e mecânicas de um computador: placas de vídeo, som, impressora, modem, placa-mãe e fonte de alimentação. Significa literalmente "partes pesadas".

HIPERTEXTO

Forma de apresentação da informação em que imagem, texto, som e outras mídias estão ligados, de modo que o usuário possa utilizá-los a qualquer momento e em qualquer ordem, bastando para isso clicar com o mouse sobre um de seus elementos, em geral destacados por uma cor diferente da cor do resto do texto.

HTML

Sigla de *Hypertext Markup Language* (Linguagem Marcada em Hipertexto). Trata-se da linguagem utilizada para criar páginas com hipertextos que são exibidas na Web.

HUB

Concentrador. É um dispositivo que une linhas de comunicação em um local central, fornecendo uma conexão comum a todos os dispositivos da rede

KBPS

Kilobits por segundo. Medida de transferência de dados ou velocidade de rede. Equivale a 1000 bits por segundo

LAN

Sigla de *Local Area Network* (Rede de Área Local). Trata-se de um sistema de comunicação entre computadores instalados em um mesmo escritório ou edifício. Graças a esse tipo de rede é possível a várias pessoas compartilhar dos mesmos periféricos (de uma mesma impressora, por exemplo) e acessar as mesmas informações. Normalmente utilizada nas empresas para interligação local dos seus computadores. Existem várias tecnologias que permitem a realização de uma rede local, sendo as mais importantes, a Ethernet e o Token Ring

LINK

Elo ou Ligação. Conexão entre um elemento de um documento de hipertexto, como uma palavra, expressão, símbolo ou imagem, e outro elemento do documento, outro documento de hipertexto, um arquivo ou um script. O usuário ativa o vínculo dando um clique sobre o elemento vinculado, que é geralmente sublinhado ou apresentado em uma cor diferente do restante do documento para indicar que o elemento está vinculado. Os links são indicados em um documento de hipertexto através de tags de linguagens de marcação, como a SGML e a HTML. Em geral, essas tags não são visíveis ao usuário.

LOGIN

Identificação de um usuário em um computador. Acesso a um computador via rede para execução de comandos. Para todos os efeitos, o computador local que "loga" em um servidor ou host.

MODEM

Contração de *Modulador-Demodulador*. Conversor de sinais analógicos (linha telefônica) em sinais digitais (microcomputador) e vice-versa. Dispositivo de hardware usado para conectar dois sistemas de computadores e transferir dados através de uma linha telefônica.

PLACA-MÃE

Também chamada de *motherboard*. É a unidade que contém todos os elementos básicos para o funcionamento de um computador. Na placa-mãe estão a CPU, as placas de memória, de som, de vídeo, modem, etc.

PLACA DE COMUNICAÇÃO

Dispositivo de Hardware utilizado para comunicar o micro a outro micro ou a uma rede. Podem ser placa de FAX/Modem, placa de Rede, placas USB ou até mesmo pode-se usar as portas de comunicação serial, paralela ou infra-vermelho para tal comunicação.

REDE

Conjunto de dispositivos conectados entre si, através de cabos ou linhas telefônicas que partilham os mesmos recursos como impressoras ou unidades de disco. O mesmo que network.

SOFTWARE

Conjunto de instruções que, carregadas no computador, fazem com que este execute diversas tarefas. Os programas feitos para você trabalhar no computador, como sistemas operacionais, processadores de texto, aplicativos, utilitários, jogos.

Referências Bibliográficas

ALBUQUERQUE, Fernando. **TCP/IP Internet: Protocolos & Tecnologias**. 2ª ed. Rio de Janeiro: Ed. Axcel Books, 1999.

ASUS. **Products: Motherboard**. Disponível em: <http://www.asus.com/products/mb/mb_archives.htm>. Acesso em: 28 Julho 2000.

ATSERVIÇOS. **Dicas – Configurando Corretamente o Sistema Operacional**. Funções Esquecidas da Placa Mãe. Disponível em: <<http://www.atservicos.hpg.ig.com.br/membros/doc/dicas.htm>>. Acesso em: 18 junho 2002.

BRISA & EMBRATEL. **Arquitetura de redes de computadores: OSI e TCP/IP**. 2ª ed. São Paulo: Ed. Makron Books, 1997.

COMER, Douglas E. **Internetworking with TCP/IP: Principles, protocols and architectures**. 4ª ed. Upper Siddle River: Ed. Prentice Hall, 2000.

CONECTIVA. **Conectiva Linux**. Disponível em: <<http://www.conectiva.com.br>>. Acesso em: 21 maio 1999.

CYCLADES. **Guia Internet de Conectividade**. 4ª ed. São Paulo: Cyclades do Brasil, 1997.

DERFLER Jr.; FRANK J. **Guia da conectividade**. Tradução: Insught Serviços de Informática. São Paulo: Ed. Campus, 1993.

INFO Exame. **100 Super Sites**. São Paulo: Ed. Abril, N.º 191, p. 106-107, 2002.

INFO Exame. **Rede: Você ainda vai ter uma**. São Paulo: Ed. Abril, N.º 192, p. 40-70, 2002.

INTEL Corporation. **Fundamentos de Rede**. 1ª ed. São Paulo: INTEL Corporation, 1997.

INTEL Corporation. **Mobile Wired for Management**. Disponível em: <http://oem.intel.com/oem/education/docs/mobile_wfm.ppt>. Acesso em: 12 Julho 2000.

INTERNET. BR. **5 Edições em uma**. Rio de Janeiro: Ediouro Publicações, N.º 54, 55, 56, 57 e 58, 2000-2001.

MARTIN, Chuck. **O Patrimônio Digital: Estratégias para competir, sobreviver e prosperar em um mundo interligado pela Internet**. São Paulo: Ed. Makron Books, 1998.

MICROSOFT. **Networking essentials**. 2ª ed. Redmond: Microsoft Press, 1997.

PCCHIPS. **Products**. Disponível em: <<http://www.pcchips.com.tw/product.html>>. Acesso em: 12 Julho 2000.

PC Master. **Edição especial de Aniversário: Redes**. São Paulo: Ed. Europa, N.º 25, p. 40-49, 1999.

PCS. **Custo vs. Performance: Redes Locais Peer-to-Peer**. São Paulo, N.º 04, p. 40-49, 1999.

PERLMAN, Radia. **Interconnections**. 2ª ed. Reading: Ed. Addison-Wesley, 2000.

SOARES, Luis Fernando et al. **Redes de computadores: Das LANs, MANs e WANs às redes ATM**. 4ª ed. São Paulo: Ed. Campus, 1995.

SYMANTEC Corporation. **Guia do usuário do Symantec pcAnywhere**. Cupertino: Symantec Corporation, 2001.

SYMANTEC Corporation. **pcAnywhere – Symantec**. Disponível em: <<http://www.symantec.com.br/region/br/product/pca/features.html>>. Acesso em: 22 junho 2002.

SYMANTEC Corporation. **pcAnywhere 10.0.1 Build 354**. Copyright 2001 by Symantec Corporation.

TANEMBAUM, Andrew S. **Redes de Computadores**. Rio de Janeiro: Ed. Campus, 1994.

TORRES, Gabriel. **Redes de Computadores: Curso Completo**. Rio de Janeiro: Ed. Axcel Books, 2001.

TORRES, Gabriel. **Redes Locais | Clube do Hardware**. Disponível em: <<http://www.gabrieltorres.com/redes.html#20>> Acesso em: 25 junho 2002.

UNIVERSIDADE FEDERAL DE SANTA CATARINA. Biblioteca Universitária. Serviço de Referência. Catálogos de Universidades. Apresenta endereços de Universidades nacionais e estrangeiras. Disponível em: <<http://www.bu.ufsc.br>>. Acesso em: 19 junho 2002.

WANG, Charles B. **Tecno Vision II**. São Paulo: Ed. Makron Books, 1997.